TUGAS AKHIR – KS 141501

EVALUASI KEAMANAN APLIKASI SISTEM INFORMASI MAHASISWA MENGGUNAKAN FRAMEWORK VAPT (STUDI KASUS : SISTER UNIVERSITAS JEMBER)

EVALUATION OF STUDENT INFORMATION SYSTEM APPLICATION SECURITY USING VAPT *FRAMEWORK* (CASE STUDY: SISTER UNIVERSITAS JEMBER)

AHMAD FIKRI ZULFI
NRP 5213 100 154

Dosen Pembimbing :
Bekti Cahyo Hidayanto, S. Si., M. Kom.

JURUSAN SISTEM INFORMASI
Fakultas Teknologi Informasi
Institut Teknologi Sepuluh Nopember
Surabaya 2017

TUGAS AKHIR – KS 141501

EVALUASI KEAMANAN APLIKASI SISTEM INFORMASI MAHASISWA MENGGUNAKAN FRAMEWORK VAPT (STUDI KASUS: SISTER UNIVERSITAS JEMBER)

AHMAD FIKRI ZULFI
NRP 5213 100 154

Dosen Pembimbing :
Bekti Cahyo Hidayanto, S. Si., M. Kom.

JURUSAN SISTEM INFORMASI
Fakultas Teknologi Informasi
Institut Teknologi Sepuluh Nopember
Surabaya 2017

FINAL PROJECT – KS 141501

EVALUATION OF STUDENT INFORMATION SYSTEM APPLICATION SECURITY USING VAPT *FRAMEWORK* (CASE STUDY: SISTER UNIVERSITAS NEGERI JEMBER)

AHMAD FIKRI ZULFI
NRP 5213 100 154

Dosen Pembimbing:
Bekti Cahyo Hidayanto, S.Si., M. Kom.

JURUSAN SISTEM INFORMASI
Fakultas Teknologi Informasi
Institut Teknologi Sepuluh Nopember
Surabaya 2016

LEMBAR PENGESAHAN

EVALUASI KEAMANAN APLIKASI SISTEM INFORMASI MAHASISWA MENGGUNAKAN FRAMEWORK VAPT(STUDI KASUS: SISTER UNIVERSITAS JEMBER)

TUGAS AKHIR

Disusun untuk Memenuhi Salah Satu Syarat
Memperoleh Gelar Sarjana Komputer
pada
Departemen Sistem Informasi
Fakultas Teknologi Informasi
Institut Teknologi Sepuluh Nopember

Oleh:

AHMAD FIKRI ZULFI
5213 100 154

Surabaya, Juli 2017

KEPALA
DEPARTEMEN SISTEM INFORMASI

Dr. Ir.Aris Tjahyanto, M. Kom.

NIP 19650310199102001

LEMBAR PERSETUJUAN

EVALUASI KEAMAN APLIKASI SISTEM INFORMASI MAHASISWA MENGGUNAKAN FRAMEWORK VAPT (STUDI KASUS: SISTER UNIVERSITAS JEMBER)

TUGAS AKHIR

Disusun Untuk Memenuhi Salah Satu Syarat
Memperoleh Gelar Sarjana Komputer
pada
Jurusan Sistem Informasi
Fakultas Teknologi Informasi
Institut Teknologi Sepuluh Nopember

Oleh :

AHMAD FIKRI ZULFI
NRP. 5213 100 154

Disetujui Tim Penguji : Tanggal Ujian : 5 Juli 2017
Periode Wisuda : September 2017

Bekti Cahyo Hidayanto, S.Si., M.Kom. **(Pembimbing I)**

Dr.Eng Febriliyan Samopa, S.Kom., M.Kom. **(Penguji I)**

Hatma Suryotrisongko, S.Kom, M.Eng **(Penguji II)**

EVALUASI KEAMANAN APLIKASI SISTEM INFORMASI MAHASISWA MENGGUNAKAN FRAMEWORK VAPT (STUDI KASUS: SISTER UNIVERSITAS JEMBER)

NAMA : **AHMAD FIKRI ZULFI**
NRP : **5213100154**
JURUSAN : **Sistem Informasi FTIF-ITS**
DOSEN PEMBIMBING : **Bekti Cahyo H., S.Si., M.Kom.**

ABSTRAK

Aplikasi sistem informasi berbasis website seperti, Sistem Informasi Terpadu Universitas Jember tidak lepas dari celah – celah keamanan yang dapat disalahgunakan oleh orang yang tidak berhak. Penyalahgunaan tersebut dapat merugikan institusi baik fisik maupun non fisik. Kerugian dapat menyebabkan sistem dan proses bisnis di Universitas Jember yang sudah berbasis IT menjadi terhenti.

Untuk melakukan identifikasi celah keamanan digunakan framework VAPT (Vulnerability Assessment & Penetration Testing). Pada proses Vulnerability Assessment akan digunakan metode automated testing yang menggunakan tools bantuan, yaitu dengan menggunakan Acunetix, OWASP ZAP, Burp Suite, Nessus, dan W3af. Pada proses Penetration Testing akan menggunakan metode Blackbox Testing.

Dari hasil pengujian yang telah dilakukan, penulis menemukan beberapa celah yang dapat mengganggu keamanan Sister Universitas Jember. Namun, dari celah yang telah ditemukan tersebut tidak didapatkan hak akses. Hal tersebut menunjukkan keamanan Sister cukup baik. Kemudian pada tugas akhir ini, penulis merumuskan rekomendasi perbaikan terkait celah yang ditemukan agar nantinya dapat diperbaiki oleh pihak Universitas Jember.

Keywords: Evaluasi keamanan sistem informasi, Eksploitasi, VAPT

EVALUATION OF STUDENT INFORMATION SYSTEM APPLICATION SECURITY VAPT FRAMEWORK (CASE STUDY: SISTER UNIVERSITAS NEGERI JEMBER)

NAME	**: AHMAD FIKRI ZULFI**
NRP	**: 5213100154**
DEPARTMENT	**: Sistem Informasi FTIF-ITS**
SUPERVISOR	**: Bekti Cahyo H., S.Si., M.Kom.**

ABSTRACT

Application of website-based information systems such as, Universitas Negeri Jember Integrated Information System can not be separated from the holes that can be abused by unauthorized people. Such abuse can harm both physical and non-physical institutions. Losses can lead to systems and business processes at the IT-based Universitas Negeri Jember being stalled.

To identify the vulnerabilities, author used VAPT framework (Vulnerability Assessment & Penetration Testing). In the Vulnerability Assessment process, author will use the automated testing method using Acunetix, OWASP ZAP, Burp Suite, Nessus, and W3af. In Penetration Testing process will use Blackbox Testing method.

From the results of tests that have been done, the authors found some holes that can interfere with the security of Sister University of Jember. It shows Sister's security quite well. Then in this thesis, the authors formulated recommendations for improvements related to the holes found so that later can be repaired by the University of Jember.

Keywords: Information systems security testing, Exploitation, VAPT

KATA PENGANTAR

Puji syukur kepada Allah SWT atas segala petunjuk, pertolongan, berkah, kasih saying, serta kekuatan yang diberikan-Nya, sehingga penulis dapat menyelesaikan laporan tugas akhir dengan Judul **Evaluasi Keamanan Aplikasi Sistem Informasi Mahasiswa Menggunakan Framework VAPT (Studi Kasus: Universitas Jember).** Adapun tugas akhir ini disusun untuk menyelesaikan gelar sarjana di Jurusan Sistem Informasi, Fakultas Teknologi Informasi, Institut Teknologi Sepuluh Nopember Surabaya.

Penulis tak lupa untuk mengucapkan seluruh pihak yang sangat membantu dalam proses pelaksanaan penelitian ini, yaitu:

- Untuk keluarga saya yang telah membesarkan dan mendidik saya, serta mendukung setiap kegiatan yang saya ikuti
- Untuk Wakil Rektor 1 dan Kepala UPT TI Universitas Negeri Jember yang telah memberikan izin, informasi, serta pengetahuan selama Penelitian
- Untuk Bapak Dr. Ir. Aris Tjahyanto, M. Kom., selaku Ketua Jurusan Sistem Informasi ITS, yang telah menyediakan segala fasilitas untuk kebutuhan penelitian mahasiswa

- Untuk Dosen Pembimbing, yaitu Bapak Bekti Cahyo Hidayanto, S.Si., M. Kom., atas semua waktu, ilmu pengetahuan, dan dukungan yang sangat bermanfaat untuk peniliti
- Untuk para Dosen Penguji, yaitu Dr.Eng. Febriliyan Samopa, S. Kom., M. Kom. dan Faisal Mahananto, S. Kom, M. Eng, Ph.D atas segala masukan, kritik, dan saran yang membangun dalam rangka menjamin kualitas penelitian yang diaksanakan
- Untuk Bapak Sholiq ST., M. Kom., selaku dosen wali yang selalu memberi masukan, pengalaman, dan bimbingan untuk peneliti
- Untuk teman – teman dekat yaitu Clarisa, Yusuf, Andika, Edo, Adit, Lugas, Habibi, dan Pandu, yang selalu memberi dukungan, motivasi, masukan dan pengalaman terbaik selama masa perkuliahan.
- Untuk seluruh pihak yang tidak dapat disebutkan satu-persatu di dalam buku ini

Penulis berharap semoga Tugas Akhir yang telah disusun sedemikian rupa ini dapat bermanfaat bagi pihak terkait, baik itu Universitas Negeri Jember, Almamater, maupun pihak – pihak lain yang terkait dengan penelitian ini, baik dalam pelaksanaan penelitian maupun penelitian selanjutnya.

DAFTAR ISI

(Halaman ini sengaja dikosongkan)

DAFTAR GAMBAR

DAFTAR TABEL

BAB I
PENDAHULUAN

Pada bab ini akan menjelaskan tentang beberapa hal terkait latar belakang, rumusan masalah, batasan masalah, tujuan tugas akhir, manfaat tugas, dan relevansi dari tugas akhir. Adanya Penjelasan tersebut diharapkan dapat memahami gambaran umum permasalahan tugas akhir serta pemecahannya.

1.1. Latar Belakang

Teknologi di bidang informasi dan komunikasi telah berkembang sangat cepat, salah satu dari perkembangan tersebut adalah terciptanya komputer. Komputer merupakan alat bantu manusia dalam melakukan berbagai macam hal, seperti penggunaan internet melalui komputer sebagai suatu sarana berbagi informasi yang tidak terbatas ruang dan waktu. Kemajuan teknologi ini tidak hanya digunakan oleh individu saja namun juga digunakan oleh berbagai organisasi seperti organisasi pendidikan. Organisasi pendidikan telah banyak menggunakan berbagai macam perangkat teknologi informasi baik saat proses belajar mengajar maupun saat mengolah berbagai macam data dan informasi. Hal ini dapat dibuktikan dimana setiap organisasi pendidikan di Indonesia telah menggukan sistem informasi berbasis *web application*.

Pemanfaatan sistem informasi untuk aktivitas organisasi pendidikan seperti perguruan tinggi dapat menjadi faktor penunjang kesuksesan dan kemajuan dari perguruan tinggi seperti mengatur perkuliahan, dosen, dan nilai mahasiswa [1].

Pemanfaatan sistem informasi ini tidak serta merta mempermudah proses bisnis dari perguruan tinggi. Perlu disadari bahwa penggunaan sistem informasi berbasis *web application* memiliki kelemahan – kelemahan keamanan yang dapat dieksploitasi oleh pihak luar melalui jaringan internet. Apabila hal ini terjadi, maka organisasi dapat mengalami berbagai macam kerugian. Eksploitasi yang dimaksud adalah penyalahgunaan wewenang dalam mengakses informasi, seperti merubah informasi yang ada atau bahkan menghapus informasi – informasi penting yang ada di dalam *web application*.

Pada tahun 2014, Symantec Internet Security Threat Report 2014 (ISTR) mengemukakakn bahwa [2] terdapat 6.549 kerentanan baru yang sebenarnya menurun dari tahun sebelumnya yaitu sebanyak 6.787. Hal ini tetap harus menjadi pertimbangan setiap administrator website dalam menjaga informasi yang terdapat pada *web application.* Hal lain yang perlu diperhatikan adalah pada tahun 2013 angka *Web Attack Blocked per Day* sebanyak 569.000 dan pada tahun berikutnya angka ini menurun yaitu menjadi 493.000. Hal ini menunjukan mundurnya tingkat keamanan web pada tahun 2014. Kondisi ini perlu menjadi perhatian bagi organisasi pengguna *web application* seperti perguruan – perguruan tinggi.

Sebagai salah satu perguruan tinggi di Indonesia, Universitas Negeri Jember telah menerapkan sistem informasi berbasis web, yaitu SISTER UNEJ. SISTER adalah singkatan dari Sistem Informasi Terpadu, yang digunakan dalam rangka

menunjang proses bisnis dari universitas sendiri. Namun hingga saat ini Sistem Informasi Terpadu yang digunakan UNEJ belum pernah dilakukan uji keamanannya. Seperti yang telah dijabarkan sebelumnya, bahwa setiap *web application* memiliki celah yang dapat dieksploitasi oleh pihak luar, sehingga timbul kekhawatiran akan terjadinya eksploitasi pada celah yang ada pada SISTER UNEJ.

Berangkat dari hal ini lah, penulis ingin melakukan evaluasi terhadap keamanan web sistem informasi mahasiswa Universitas Jember. Untuk melakukan evaluasi keamanan, maka penulis akan melakukan pengujian *Penetration Testing*. *Penetration Testing* sendiri adalah pengujian evaluasi keamanan dengan cara melakukan simulasi penyerangan terhadap web. Penulis akan menggunakan kerangka kerja VAPT [3] dalam melakukan simulasi penyerangan yang nantinya juga akan disesuaikan dengan kebutuhan dari penelitian

1.2. Perumusan Masalah

1. Apa saja celah keamanan yang ada ditemukan pada aplikasi web Sistem Informasi Terpadu Universitas Jember?
2. Bagaimana dampak kerusakan sistem dari celah keamanan yang dapat ditimbulkan dengan adanya eksploitasi celah keamanan tersebut?
3. Bagaimana solusi untuk memperbaiki celah keamanan tersebut?

1.3. Batasan Masalah

Pada penelitian terdapat beberapa batasan masalah, yaitu:

1. Penelitian dilakukan pada aplikasi web Sistem Informasi Terpadu Universitas Jember(https://sister.unej.ac.id).
2. Penelitian ini tidak mencakup *social engineering*.
3. Penelitian dilakukan dengan mengacu pada kerangka kerja *Vulnerability Assesment & Penetration Testing.*
4. Penelitian dilakukan di dalam ataupun di luar jaringan internet milik Universitas Jember.
5. Kesimpulan hasil *penetration test* berupa usulan solusi yang dapat dijadikan sebagai bahan pertimbangan untuk perbaikan sistem.
6. Hasil penelitian berupa laporan tertulis.

1.4. Tujuan Tugas Akhir

Penelitian tugas akhir ini bertujuan untuk mengevaluasi aplikasi berbasis web Sistem Informasi Mahasiswa milik Universitas Jember dari segi keamanan informasi, serta memberikan rekomendasi usulan solusi untuk memperbaiki celah keamanan yang ditemukan.

1.5. Manfaat Tugas Akhir

Penelitian tugas Akhir ini diharapkan dapat membantu Universitas Jember dalam mengevaluasi aplikasi web Sistem Informasi Mahasiswa dari perspektif keamanan informasi. Selain itu, penelitian ini juga dapat diharapkan sebagai bahan pertimbangan dalam pengembangan institusi terkait dengan keamanan informasi, baik secara teknis maupun non teknis.

1.6. Relevansi Tugas Akhir

Usulan Tugas Akhir yang diajukan oleh penulis berdasarkan ilmu pengetahuan mengenai keamanan informasi,

yang telah diajarkan dalam mata kuliah Keamanan Aset Informasi pada semester 4. Sehingga dapat disimpulkan bahwa Usulan Tugas Akhir yang diajukan penulis sesuai dengan ranah penelitian Sistem Informasi.

Selain relevansi dengan ranah penelitian Sistem Informasi, perlu dibuktikan adanya relevansi antara penelitian yang akan dilakukan dengan ranah penelitian yang ada pada laboratorium Infrastruktur dan Keamanan Teknologi Informasi IKTI), yang terletak pada Jurusan Sistem Informasi Institut Teknologi Sepuluh Nopember Surabaya. Yaitu ranah penelitian tentang keamanan teknologi informasi sesuai dengan nama Laboratorium IKTI. Sehingga dapat disimpulkan bahwa Topik Tugas Akhir yang penulis ajukan merupakan topik untuk laboratorium IKTI.

(Halaman ini sengaja dikosongkan)

BAB II
TINJAUAN PUSTAKA

2.1. Studi Sebelumnya

Pada bagian ini peneliti akan melakukan pembahasan mengenai penelitian sebelumnya yang serupa dan memiliki relevansi terhadap penelitian Tugas Akhir yang sedang dikerjakan. Adapun isi – isi penelitian tersebut nantinya dapat dijadikan sebagai referensi untuk tugas akhir yang dijelaskan pada tabel 2.1.

Table 2.1 Penelitian Sebelumnya

Penulis	Judul	Metodologi	Kekurangan	Hasil Penelitian
Jai Narayan Goel & B.M. Mehtre	Vulnerability Assessment & Penetration Testing as a Cyber Defence Technology	Vulnerability Analysis & Penetration Testing	Pada paper tersebut penulis hanya menjabarkan metode VAPT, tidak melakukan implementasi pada	Penulis menyatakan bahwa teknik VAPT merupakan teknologi pertahan *cyber* yang efektif.

			suatu sistem.	
Robert Vibhandik & Arjit Kumar Bose	Vulnerability Assessment of Web Applications – A Testing Approach	Vulnerability Assessment	Pada paper penulis hanya melakukan identifikasi celah yang ditemukan dengan tools w3af dan Nikto.	Penulis mengemukakan pendekatan baru dalam melakukan pengujian celah keamanan dengan beberapa fase testing.

2.2. Dasar Teori

2.2.1. Sister UNEJ

Sister (Sistem Informasi Terpadu) Universitas Jember adalah suatu sistem informasi yang digunakan Universitas Jember dalam membantu proses bisnisnya. Pada Sister dapat ditemui banyak fungsi yang sangat krusial terhadap proses belajar mengajar seperti memilih kelas, memilih jadwal, melihat nilai, mengisi kuisioner dosen dan sebagainya. Untuk pihak dosen sendiri, dosen dapat menginputkan jadwal kelas, nilai, dan melihat hasil kuisioner dari kinerja dosen itu sendiri. Sister dapat digunakan pada Android dan IOS karena sudah terdapat aplikasi mobilenya.

2.2.2. Penetration Testing

Menurut Engebretson [3], *Penetration Testing* merupakan sebuah percobaan yang legal dan diijinkan untuk melakukan eksploitasi terhadap sebuah sistem dengan tujuan meningkatkan kualitas keamanan dari sistem tersebut. Dengan kata lain, *Penetration Testing* merupakan sebuah aktivitas pengujian keamanan dari sebuah sistem. Dari hasil pengujian tersebut, didapatkan sejumlah celah keamanan pada sistem yang kemudian menjadi bahan rekomendasi kepada organisasi yang memiliki sistem tersebut untuk dibenahi.

Adapun istilah *Penetration Testing* seringkali disalahartikan sebagai *Vulnerability Analysis*. Dalam *Vulnerability Analysis*, dilakukan proses pemeriksaan terhadap sebuah sistem untuk memastikan keberadaan kemungkinan celah keamanan. Sedangkan dalam proses *Penetration Testing*, dilakukan simulasi berupa penyerangan terhadap sistem layaknya dilakukan oleh seorang *hacker* untuk memastikan adanya celah keamanan tersebut. Sehingga dapat disimpulkan bahwa *Penetration Testing* merupakan kelanjutan dari *Vulnerability Analysis*.

Secara umum, terdapat beberapa tujuan utama dari dilakukannya *Penetration Testing* sebagaimana dicatat oleh EC – Council [4], yaitu:

- Menguji tingkat efisiensi dari proses perlindungan informasi yang dilakukan oleh organisasi

- Memberikan pandangan kepada organisasi mengenai celah keamanan sistem miliknya ketika dieksploitasi secara internal maupun eksternal
- Menyediakan informasi bagi tim pelaksana audit
- Meminimalisir biaya pelaksanaan audit keamanan
- Membantu proses prioritisasi dari organisasi untuk membenahi sistem yang diuji
- Mengetahui risiko apa saja yang ada pada sistem milik organisasi
- Mengevaluasi tingkat efisiensi perangkat yang digunakan, misalnya *firewall*, *router*, dan sebagainya
- Memberikan gambaran mengenai apa yang harus dilakukan untuk mencegah terjadinya eksploitasi
- Mengetahui apakah diperlukan pergantian ataupun pembaharuan dari infrastruktur sistem, baik *hardware* maupun *software*

Adapun terdapat beberapa metodologi yang dapat digunakan untuk melakukan *Penetration Testing*. Salah satu dari metodologi tersebut adalah VAPT (*Vulnerability Assessment and Penetration Testing*), yang akan digunakan dalam pengerjaan penelitian tugas akhir.

2.2.3. Vulnerability

Vulnerability merupakan suatu celah yang memungkinkan seseorang ataupun sekelompok orang untuk masuk dan mendapatkan hak akses kedalam komputer yang dituju (target). Biasanya vulnerability adalah kelemahan yang

disebabkan oleh kesalahan setting ataupun ataupun kelalaian administrator.

Adanya vulnerability kemudian memunculkan upaya-upaya untuk melakuan ekploitasi bagaimana mengetahui vulnerabilitas sebuah sistem komputer. Untuk itulah ada yang disebut dengan Exploit. Dalam hal ini Exploit adalah sebuah aktivitas untuk menyerang keamanan komputer secara spesifik. Exploit banyak digunakan untuk penetrasi baik secara legal ataupun ilegal untuk mencari kelemahan (Vulnerability) pada komputer.

2.2.4. Vulnerability Assessment & Penetration Testing (VAPT)

Vulnerability Assessment & Penetration Testing (VAPT) adalah suatu metodologi dalam melakukan uji keamanan terhadap suatu sistem *web application*. VAPT merupakan gabungan dari dua aktivitas yaitu, *Vulnerability Assessment* dan *Penetration Testing*. *Vulnerability Testing* merupakan aktivitas yang meliputi proses pemeriksaan sebuah celah atau kelemahan dari suatu *web application*. Sedangkan *Penetration Testing* adalah suatu proses simulasi penyerangan terhadap celah yang terdapat pada *web application* dan mengeksploitasinya.

Pada proses pengujian dengan metode VAPT [3], terdapat 9 tahapan pengerjaan yang perlu dilakukan. Penjabaran 9 tahapan tersebut dapat dilihat pada gambar 2.1.

Gambar 2.1 Tahapan Metodologi VAPT

Pada tahapan pertama yaitu penentuan ruang lingkup pengujian. Tahap ini menentukan sistem apa yang akan diuji tingkat keamanannya serta batasan – batasan yang penguji perlu sepakati dengan organisasi terkait. Selain itu pada tahap ini juga menentukan teknik apa yang nantinya akan digunakan untuk melakukan *Vulnerability Testing* dan *Penetration Testing*. Berikut adalah teknik – teknik yang dapat digunakan sesuai dengan kebutuhan dari pengujian.

2.2.4.1 Vulnerability Assessment

- *Static Analysis*

  Static Analysis adalah teknik dimana penguji tidak menjalankan scenario pengujian apapun. Dalam teknik ini, penguji melakukan pemeriksaan komponen dari sistem yang akan diuji, seperti struktur kode hingga dokumentasi dari sistem yang tersedia. Pengujian dengan teknik ini tidak memberikan dampak terhadap

sistem, karena tidak adanya tindakan eksploitasi. Kelemahan terbesar dari teknik ini adalah durasi pengerjaannya yang lama dan tingkat human error yang cukup tinggi.

- *Manual Testing*
  Manual Testing adalah teknik dimana penguji tidak memerlukan perangkat bantu apapun. Penguji hanya memanfaatkan pengetahuan dan pengalamannya untuk menemukan dimana celah keamanan pada sebuah sistem *web application*. Pengujian dengan teknik ini tidak memakan biaya yang relatif besar, namun membutuhkan waktu yang cukup lama dan effort yang cukup besar.
- *Fuzz Testing*
  Fuzz Testing adalah teknik pengujian dimana penguji akan memasukkan data acak yang tidak valid. Dari hasil input tersebut akan diperiksa apakah terjadi *error* pada sistem, yang dapat diidentifikasi lebih lanjut sebagai salah satu celah keamanan sistem.
- *Automated Testing*
  Automated Testing adalah teknik pengujian dimana pengujiannya memanfaatkan bantuan tools perangkat lunak (*software*). Perangkat lunak tersebut membantu penguji dalam mengidentifikasi celah – celah keamanan yang ada pada suatu sistem. Terdapat beberapa perangkat lunak yang dapat digunakan dalam teknik pengujian ini yang dijelaskan pada tabel 2.2.

Tabel 2.2. Contoh software pengujian

Nama Perangkat	Kegunaan	Platform
W3af	*Vulnerability Scanner*	Linux, UNIX, Windows, Mac OS X
OWASP ZAP	*Vulnerability Scanner*	Linux, UNIX, Windows, Mac OS X
Metasploit	Mengendalikan komputer target dari jarak jauh	Linux, UNIX, Windows, Mac OS X
Nmap/Zenmap	Deteksi *port* yang dibuka, deteksi *web server*	Linux, UNIX, Windows, Mac OS X

2.2.4.2 Penetration Testing

- *Black box testing*

  Black box testing adalah teknik yang menggunakan keahlian dari penguji untuk melakukan serangkaian penyerangan terhadap suatu sistem. Pada skenario teknik pengujian ini, penguji bertindak sebagai *hacker* yang melakukan penyerangan dari dalam maupun luar

jaringan sistem. Dalam hal pengujian ini, penguji tidak memiliki informasi tentang sistem yang akan diserang, baik itu akses, topologi jaringan, konfigurasi sistem dan informasi tentang sistem lainnya. *Black box testing* dapat dilakukan di luar ataupun dari dalam wilayah sistem berada.

- *White box testing*
  White box testing adalah teknik yang membutuhkan informasi tentang sistem yang akan diuji. Informasi tersebut berupa infrastruktur, arsitektur jaringan, kode sistem, dan sebagainya. Pada umumnya pengujian ini dilakukan didalam wilayah sistem yang diuji berada.
- *Grey box testing*
  Grey box testing adalah merupakan kombinasi dari kedua teknik yang telah disebutkan diatas. Pada pelaksanaannya, penguji diberikan informasi secara terbatas, serta memiliki hak akses yang sama dengan pengguna sistem pada umumnya.

Pada tugas akhir ini, penulis akan menggunakan metode *Automated Testing* pada tahap *Vulnerabiliity Assessment*. Metode ini penulis pilih dengan pertimbangan akan keakurasian tingkat pengujian serta singkatnya waktu pengerjaan karena pada *Automated Testing* menggunakan bantuan *tools* perangkat lunak. Adapun permasalahan pada biaya dapat diatasi dengan menggunakan aplikasi yang bersifat *open source*, sehingga tidak membutuhkan biaya.

Pada tahap *Penetration Testing*, penulis akan menggunakan *Black Box Testing*. Teknik ini penulis pilih dengan pertimbangan kebutuhan akan adanya simulasi penyerangan sebagai seorang *hacker* yang berada di luar sistem.

Setelah menentukan ruang lingkup dari pengujian, tahap kedua adalah tahap *Recconaisance* (pengintaian). Pada tahap ini penguji melakukan pengintaian terhadap sistem yang diuji untuk mendapatkan informasi tentang sistem seperti, sistem operasi yang digunakan, IP *address*, port apa saja yang digunakan, dan sebagainya.

Tahap selanjutnya adalah tahap *Vulnerability Detection*. Pada tahap ini, penguji akan melakukan teknik tertentu yang sesuai dengan kebutuhan untuk mendapatkan celah keamanan dari sebuah sistem. Hasil yang didapat pada tahap ini sangat menentukan penguji untuk melakukan *Penetration Testing.*

Setelah melakukan *Vulnerability Detection,* tahap berikutnya adalah *Information Analysis and Planning*. Pada tahap ini, penguji menganalisa informasi yang didapat pada tahap sebelumnya untuk membuat perencanaan dalam melakukan proses *Penetration Testing*. Rencana tersebut berisi tentang urutan celah apa saja yang akan diuji, *tools* apa yang digunakan untuk membantu pengujian, dan lain sebagainya.

Setelah melakukan *Information Analysis and Planning*, maka tahap selanjutnya *Penetration Testing*. Tujuan dari tahap ini adalah melaksanakan simulasi penyerangan terhadap sistem

yang telah direncanakan sebelumnya. Dalam pelaksanaannya, digunakan teknik pengujian yang sesuai dengan kebutuhan. Selain itu, juga digunakan perangkat bantu yang diperlukan. Jika ada hasil analisis yang terbukti ketepatannya melalui tahap ini, pengujian akan dilanjutkan pada tahap *Privilege Escalation.*

Setelah selesai melakukan *Penetration Testing*, dilakukan tahap *Privilege Escalation*. Pada tahap ini, penguji akan melakukan eksploitasi terhadap sistem. Tujuan dari eksploitasi pada tahap ini adalah untuk mendapatkan hak akses terhadap sistem dimana dalam kondisi normal akses tidak boleh didapatkan oleh pihak luar.

Tahap berikutnya adalah proses *Result Analysis*. Pada tahap ini, dilakukan analisis terhadap hasil yang didapatkan dari pengujian yang telah dilakukan. Proses analisis yang dilakukan pada Tugas Akhir ini meliputi proses penyusunan solusi – solusi yang dapat dilakukan untuk menutupi celah keamanan yang ditemukan oleh penguji.

Setelah *Result Analysis,* langkah berikutnya adalah *Clean-up*. Sebenarnya tahap ini akan dilakukan setelah tahap *Privilege Escalation* dimana penguji melakukan eksploitasi dengan mengubah pengaturan sistem, merubah data maupun menyusupkan *malware* ke dalam sistem. Pada tahap ini, penguji diharuskan untuk memperbaiki hasil eksplotasi mengembalikan keadaan sistem seperti semula sebelum dilakukan pengujian.

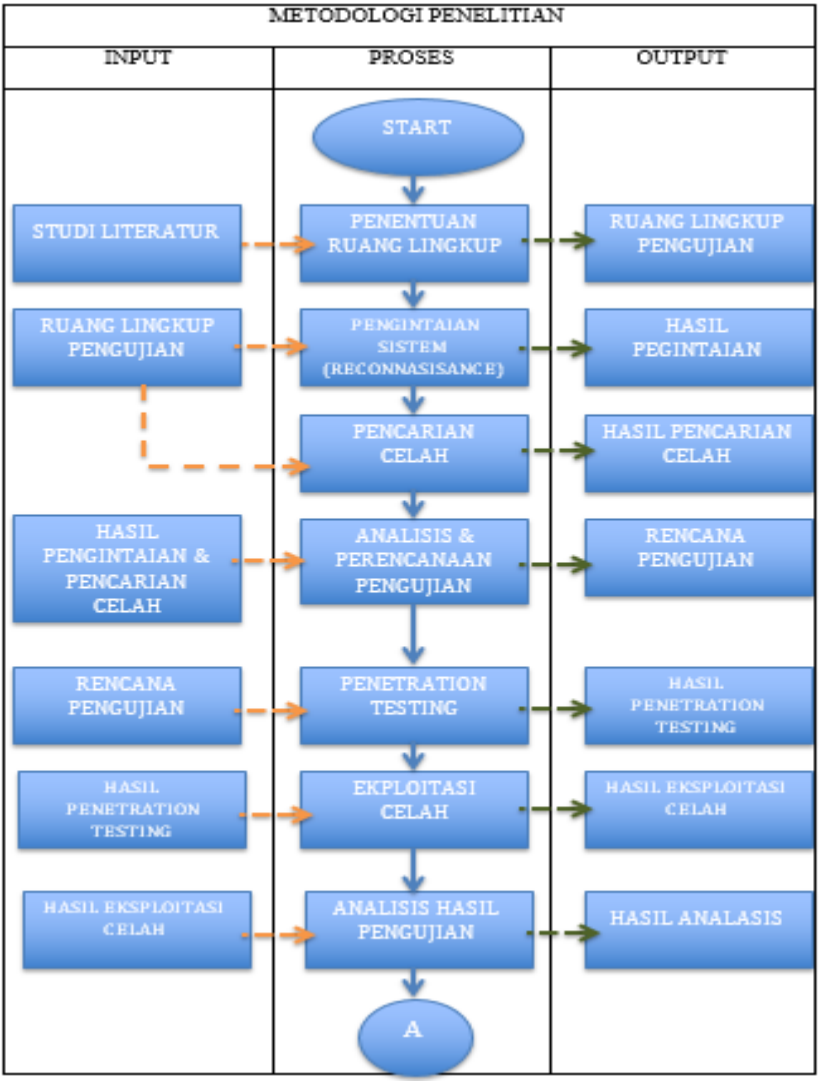
Pada tahap terakhir ini adalah *Reporting*. Pada tahap ini, penguji akan memberikan rekomendasi solusi perbaikan

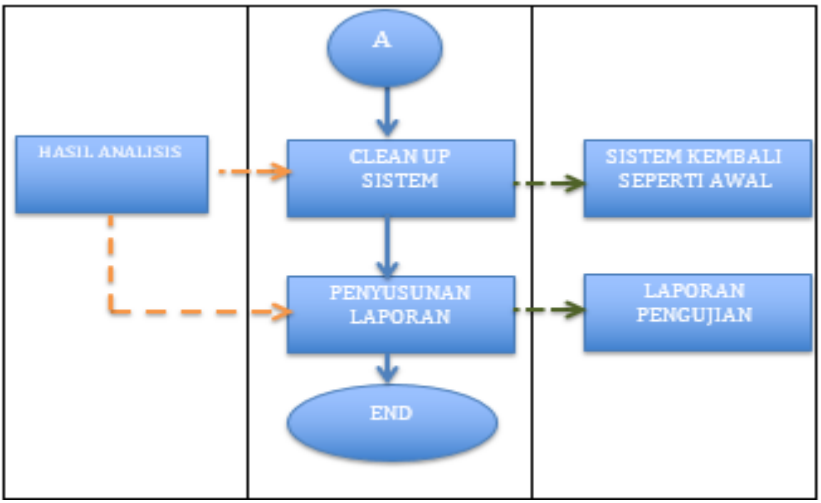
yang telah terdokumentasi dalam bentuk laporan tertulis kepada organisasi, dalam kasus ini adalah Universitas Jember. Dari hasil rekomendasi tersebut organisasi dapat melakukan tindak lanjut dengan membenahi sistem yang telah diuji.

BAB III
METODOLOGI PENELITIAN

3.1. Tahapan Metodologi

Pada bagian ini akan dijelaskan mengenai metodologi yang akan diimplementasikan dalam mengerjakan Tugas Akhir. Adapun metodologi tersebut dibutuhkan sebagai panduan sistematis dalam proses pengerjaan Tugas Akhir. Gambaran metodologi pengerjaan Tugas Akhir dapat dilihat pada gambar 3.1.


METODOLOGI PENELITIAN
INPUT
PROSES
OUTPUT
START
STUDI LITERATUR
PENENTUAN RUANG LINGKUP
RUANG LINGKUP PENGUJIAN
RUANG LINGKUP PENGUJIAN
PENGINTAIAN SISTEM (RECONNASISANCE)
HASIL PEGINTAIAN
PENCARIAN CELAH
HASIL PENCARIAN CELAH
HASIL PENGINTAIAN & PENCARIAN CELAH
ANALISIS & PERENCANAAN PENGUJIAN
RENCANA PENGUJIAN
RENCANA PENGUJIAN
PENETRATION TESTING
HASIL PENETRATION TESTING
HASIL PENETRATION TESTING
EKPLOITASI CELAH
HASIL EKSPLOITASI CELAH
HASIL EKSPLOITASI CELAH
ANALISIS HASIL PENGUJIAN
HASIL ANALASIS
A



Gambar 3.1. tahapan metodologi penelitian

3.1.1. Studi Literatur

Langkah awal yang dilakukan dalam pengerjaan Tugas Akhir ini adalah studi literatur dan fiksasi studi kasus. Studi literatur penulis lakukan untuk menentukan kerangka kerja dan tahapan – tahapan pengerjaan pengujian. Fiksasi studi kasus penulis lakukan untuk memastikan target studi kasus menyetujui ada pengujian terhadap sistem. Dari hasil kedua aktivitas tersebut akan menjadi gambaran dari ruang lingkup pengujian.

3.1.2. Menentukan Ruang Lingkup

Pada Tugas Akhir ini telah ditentukan ruang lingkup pengujian seperti yang tertera pada subbab Batasan Masalah. Pengujian akan berfokus pada software dari Sistem Informasi Terpadu Universitas Jember seperti, *Operating System, firewall, database*, web sistem informasi, dan hal lain yang berhubungan dengan software dari Sistem Informasi Terpadu. Pengujian juga akan dilakukan di dalam ataupun di luar jaringan internet milik Universitas Jember. Kerangka kerja yang digunakan pada Tugas Akhir ini adalah *Vulnerability Assessment & Penetration Testing*. Selain itu, pengujian akan dilakukan pada *clone* dari Sistem Informasi Terpadu Universitas Jember. Hal ini dilakukan agar tidak mengganggu aktivitas dari Sistem.

3.1.3. Pengintaian Sistem (Reconnaisance)

Pada tahap Pengintaian Sistem, akan dilakukan pemeriksaan awal terhadap sistem yang akan diuji. Pemeriksaan awal ini dilakukan untuk mengumpulkan informasi terkait dengan sistem seperti, *Operating System*, *IP Address*, dan Port yang dibuka pada sistem.

3.1.4. Pencarian Celah

Pada tahap Pencarian Celah ini, penguji akan melakukan proses pencarian celah dimana dalam melaksanakannya akan menggunakan bantuan *tools software*. *Software* yang digunakan nantinya akan dapat mendeteksi berbagai celah dari sebuah sistem yang diuji. Dari hasil pencarian celah

tersebut akan didapatkan daftar celah yang nantinya akan digunakan sebagai bahan untuk perencanaan pengujian tahap berikutnya. Celah yang ditemukan nantinya hanya terbatas pada hasil temuan dari *software* yang digunakan yaitu, Acunetix, ZAP, Burpsuite, W3af, dan Nessus. Pencarian Celah juga akan membandingkan dengan hasil temuan dari *vulnerability* pada data history yang terdapat pada system sebagai dasar seberapa banyak vulnerability yang ada [7]. Tahap ini biasa juga disebut dengan *Vulnerability Scanning*.

3.1.5. Analisis dan Perencanaan Pengujian

Pada tahap ini, penulis akan menganalisa dan membuat rencana pengujian dari hasil dari Pengintaian Sistem dan Pencarian Celah yang telah dilakukan sebelumnya. Analisa dan rencana ini dibuat untuk menentukan bagaimanan nantinya *Penetration Testing* berjalan.

3.1.6. Penetration Testing

Pada tahap ini, penulis akan melakukan simulasi penyerangan terhadap target pengujian yaitu Sistem Informasi Terpadu Universitas Jember. Simulasi penyerangan nantinya akan dilakukan sesuai dengan hasil dari perencanaan yang telah dibuat sebelumnya. Tujuan dari tahap ini adalah membuktikan ketepatan dari hasil celah yang telah ditemukan pada tahap Pencarian Celah.

3.1.7. Eksploitasi Celah

Setelah melakukan tahap *Penetration Testing* selanjut akan dilanjutkan pada tahap eksploitasi celah. Pada tahap ini penulis akan mencoba mengeksploitasi celah yang terdapat pada sistem. Eksplotasi disini adalah percobaan untuk merubah hak akses, mengubah informasi yang ada, mengambil informasi, menghapus informasi, merubah tampilan

3.1.8. Analisis Hasil Pengujian

Pada tahap Analisis Hasil Pengujian ini, penulis akan melakukan analisa terhadap serangkaian pengujian yang telah dilakukan. Dari hasil Pencarian Celah, Eksploitasi Celah, serta semua dampak yang disebabkan oleh celah keamanan. Dari celah tersebut nantinya akan dibuat urutan celah berdasarkan seberapa besar dampak yang diterima oleh system dengan menggunakan *software* ZAP dan Accunetix. Pada tahap ini penulis juga akan mencoba membuat rekomendasi perbaikan terhadap sistem yang bertujuan untuk menutup celah keamanan yang ada.

3.1.9. Clean Up Sistem

Pada tahap terakhir ini yaitu *Clean Up* Sistem, penulis akan melakukan pembersihan terhadap target pengujian. Pembersihan yang dimaksud adalah mengembalikan kondisi sistem sebagai target pengujian kembali seperti semula. Aktivitas pembersihan yang akan dilakukan tergantung pada sejauh mana penulis nantinya akan mengeksploitasi celah yang telah ditemukan. Selain itu

penulis juga akan menghapus semua data – data informasi penting yang penulis dapatkan selama proses pengujian. Hal ini untuk menjaga integritas dari sistem yang diuji.

3.1.10. Penyusunan Laporan Pengujian

Pada tahap ini, penulis akan menyusun laporan hasil dari pengujian yang telah dilakukan terhadap sistem. Laporan akan berisi tentang dokumentasi pengujian, hasil – hasil temuan celah yang penulis dapatkan, dan juga solusi perbaikan yang penulis rekomendasikan.

(Halaman ini sengaja dikosongkan)

BAB IV
PERANCANGAN EVALUASI

Pada bab ini, penulis akan menjelaskan tentang proses perancangan untuk mengevaluasi celah keamanan. Bab ini nantinya juga akan digunakan sebagai panduan oleh penulis dalam mengerjakan Tugas Akhir. Adapaun perancangan evaluasi yang dilaksanakan dengan mempertimbangkan kondisi terkini dari objek evaluasi, yaitu Sister Universitas Negeri Jember. Tahapan perancangan yang penilis kerjakan akan mengacu pada metodologi penelitian yang telah disusun pada bab sebelumnya.

4.1. Objek penelitian

Pengujian akan dilakukan pada Universitas Negeri Jember. Pada pengujian ini, objek yang diteliti adalah keamanan dari Sister (Sistem Informasi Terpadu) milik Universitas Negeri Jember. Dalam penelitian ini, penulis telah mendapatkan persetujuan dari pihak Universitas Negeri Jember, khususnya oleh pihak UPT TI, dimana dalam pelaksanaan pengujian evaluasi dibantu oleh Kepala UPT TI Universitas Negeri Jember.

4.1.1. Profil dan sejarah singkat UNEJ

Universitas Negeri Jember berdiri pada tanggal 9 Nopember 1964. Universitas ini awalnya merupakan Universitas Swasta yang bernama Universitas Tawang Alun. Berkat dukungan dari Bupati Jember Pada saat itu, ketiga pendiri dari Universitas Tawang Alun yaitu dr. R. Achmad, R.Th. Soengedi dan R.M

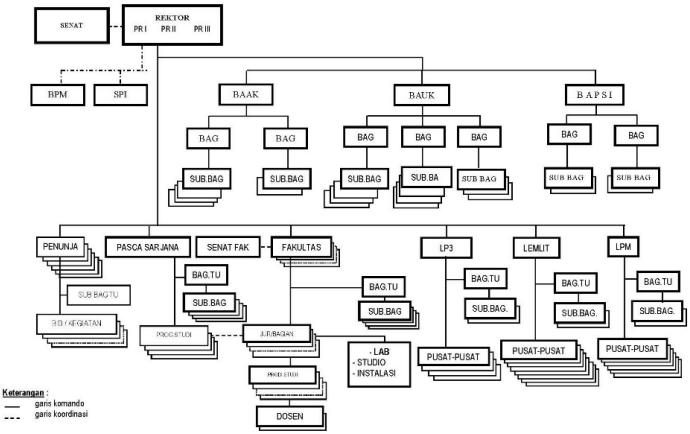
Soerachman dapat mengubah Universitas Tawang Alun menjadi Universitas Negeri Jember yang merupakan universitas negeri pertama yang ada di kabupaten Jember.

4.1.2. Sister UNEJ

Sister UNEJ (Sistem Informasi Terpadu Universitas Jember) adalah sebuah Sistem Informasi Mahasiswa yang dibuat oleh UPT TI Universitas Jember dalam membantu segala kegiatan proses bisnis dari Universitas Jember. Fungsi utama dari Sister sendiri adalah untuk mempermudah kegiatan belajar mengajar untuk dosen, mahasiswa, dan karyawan. Untuk mengakses Sister UNEJ, mewajibkan setiap user untuk melakukan login pada sso.unej.ac.id. UPT TI Universitas Jember telah menggunakan fitur *single-sign-on* terhadap setiap layanan teknologi informasi untuk mempermudah autentifikasi user.

4.1.3. Struktur Organisasi UNEJ dan UPT TI

Sebagai sebuah organisasi perguruan tingi, tentu Universitas Jember memiliki struktur dengan berbagai tingkat fungsional dalam organisasi. Rincian dari struktur organisasi Universitas Jember dan UPT TI dapat dilihat pada gambar 4.1 dan gambar 4.2.



Gambar 4.1. Struktur organisasi UNEJ

Gambar 4.2. Struktur Organisasi UPT TI

4.2. Batasan Pengerjaan

Setelah menentukan objek penelitian untuk evaluasi keamanan, penulis juga membuat perancangan Batasan pengerjaan Tugas Akhir. Tujuan dari sub bab ini adalah untuk memberikan batasan dari ranah kerja penulis dalam melakukan evaluasi celah keamanan terhadap Sister Universitas Negeri Jember. Sesuai dengan Batasan Masalah yang telah dijelaskan pada Bab I, maka dirancangan ruang lingkup batasan masalah penelitian sebagai berikut:

1. Penelitian dilakukan pada aplikasi web Sistem Informasi Terpadu Universitas Jember (https://sister.unej.ac.id)
2. Penelitian ini tidak mencakup *social engineering*.
3. Penelitian dilakukan dengan mengacu pada kerangka kerja *Vulnerability Assesment & Penetration Testing.*
4. Penelitian dilakukan di luar jaringan internet milik Universitas Jember.
5. Kesimpulan hasil *penetration test* berupa usulan solusi yang dapat dijadikan sebagai bahan pertimbangan untuk perbaikan sistem.
6. Hasil penelitian berupa laporan tertulis.

4.3. Perancangan Proses Evaluasi

Dalam pengerjaan Tugas Akhir perlu adanya perancangan proses evaluasi pada objek penelitian sesuai dengan studi kasus yang telah dibuat sebelumnya. Sesuai dengan judul dari Tugas Akhir, yaitu "Evaluasi Keamanan Sistem Informasi Mahasiswa (Studi Kasus: Sister Universitas Jember)" dirumuskan perancangan terahadap proses evaluasi Tugas Akhir yang akan dijelaskan pada sub bab berikut.

4.3.1. Pengintaian Sistem

Pada tahap Pengintaian Sistem (Reconnaisance) akan melaksanakan beberapa proses yang dilakukan untuk mengumpulkan informasi awal terkait Sister Universitas Jember. Informasi awal tersebut adalah informasi seperti Sistem Operasi, *IP Address*, *Port* yang terbuka, dan informasi lainnya berkaitan dengan Sister Universitas jember. Tujuan dari tahap ini adalah memetakan sistem dari objek evaluasi.

Dalam tahap ini, penulis menggunakan bantuan *tools* untuk melakukan pengintaian. Penulis akan menggunakan Nmap. Pada Aplikasi Nmap lebih dikhususkan untuk kegunaan *Port Scanning* dan menampilkan informasi yang lebih mendalam.

Nmap adalah aplikasi berbasis *freeware* yang menggunakan *Internet Protocol* untuk mendapatkan informasi. Informasi yang diperoleh seperti port yang terbuka dan tertutup, *traceroute* dari sistem, DNS, Topologi jaringan, dan informasi terkait jaringan lainnya.

4.3.2. Pencarian Celah

Pada tahap pencarian celah, penulis akan melakukan *Vulnerability Scanning* yaitu proses pencarian celah keamanan dari sistem objek pengujian. Dalam melakukan *Vulnerability Scanning*, penulis akan menggunakan beberapa *software* untuk membantu dalam melaksanakan *Vulnerability Scanning*. *Software – Software* tersebut nantinya akan secara otomatis melakukan pengujian terhadap keamanan suatu aplikasi. Hasil dari pengujian tersebut adalah daftar celah keamanan yang dimiliki oleh Sister Universitas Jember. Nantinya daftar celah kemanan yang ditemukan akan digunakan untuk pertimbangan

dalam melaksanakan tahap berikutnya. Adapun aplikasi yang digunakan penulis adalah sebagai berikut.

- Acunetix
  Acunetix adalah salah satu tools web *vulnerability scanner* yang telah digunakan banyak pakar *security* dan *web developer*. Tidak hanya itu, banyak perusahaan besar telah menggunakan aplikasi ini untuk mengaudit keamanan situs website yang mereka miliki. Penulis mempertimbangkan menggunakan *tools* ini karena *tools* ini mudah digunakan dan memberikan penjelasan tentang saran perbaikan terhadap kelemahan yang ditemukan.
- OWASP ZAP
  OWASP ZAP adalah *tools* keamanan *freeware* yang dikembangkan oleh ratusan *volunteers* dari seluruh dunia. *Tools* ini dirancang untuk menemukan kelemahan pada suatu *website* secara otomatis. Awalnya ZAP hanya digunakan untuk keamanan pengembangan *website*. Namun saat ini banyak pakar *security* yang telah menggunakan ZAP untuk *manual security testing*. Penulis menggunakan *tools* ini dengan pertimbangan bahwa aplikasi ini gratis dan sudah banyak orang yang menggunakan sehingga cukup familiar dan *user friendly*.
- W3af
  W3af adalah singkatan dari *Web Application Attack and Audit Framework*. W3af merupakan aplikasi open source berbasis phyton yang berfungsi sebagai

vulnerability scanner serta *exploitation tools* untuk aplikasi web. Namun untuk penelitian ini, penguji hanya menggunakan w3af sebagai *vulnerability scanner*. Penulis mempertimbangkan tools ini karena software bersifat open source dan sudah banyak digunakan oleh pakar *security IT* untuk melalukan evaluasi keamanan web.

- Burp Suite
  Burp Suite adalah aplikasi yang biasa digunakan untuk melakukan pengujian keaman sebuah web. Aplikasi ini dikembangkan oleh PortSwigger Security dan berbasis java sehingga dapat digunakan berbagai platform. Ini dikembangkan untuk memberikan solusi komprehensif untuk pemeriksaan keamanan aplikasi web. Selain fungsi dasar, seperti server proxy, pemindai dan penyusup, alat ini juga berisi opsi lanjutan seperti spider, repeater, decoder, komparator, ekstender dan sequencer.
- Nessus
  Nessus merupakan sebuah software scanning, yang dapat digunakan untuk meng-audit kemanan sebuah sistem, sepertivulnerability, misconfiguration, security patch yang belum diaplikasikan, default password, dan denial of serviceNessus berfungsi untuk monitoring lalu-lintas jaringan. Nessus awalnya merupakan aplikasi open source namun sekarang telah menjadi closed source dan dikembangkan oleh Teenable Security dan masih bersifat gratis.

Seperti yang dijelaskan sebelumnya, bahwa UPT TI telah menerapkan fitur *single-sign-on* pada Sister UNEJ, sehingga nantinya penulis akan melakukan celah terhadap dua alamat web yaitu, sso.unej.ac.id dan sister.unej.ac.id. Dari hasil tersebut juga akan dilakukan perbandingan dengan data history yang dimiliki oleh Universitas Jember.

4.3.3. Analisis dan Perencanaan Pengujian

Pada tahap Analisis dan Perencanaan Pengujian ini, penulis akan membuat rencana pengujian berdasarkan dari hasil pada dua tahap sebelumya yaitu Pengintaian Sistem dan Pencarian Celah. Hasil dari kedua tersebut akan dilakukan Analisa dan menentukan celah mana yang berdampak terhadap sistem dan perlu dilakukan eksploitasi. Pertama, penulis akan mengidentifikasi celah apa saja yang telah ditemukan dari beberapa *tools software* yang digunakan, kemudian dari hasil identifikasi, penulis akan menentukan celah apa saja yang perlu dan memungkinkan untuk dilakukan eksploitasi.

4.3.4. Penetration Testing

Pada tahap *Penetration testing,* penulis akan melakukan serangan terhadap target pengujian berdasarkan celah yang ditemukan. Penetration Testing dilakukan sebanyak dua kali pada halaman sso dan halaman utama Sister. Jika halama sso tidak dapat ditembus, maka penulis akan melakukan sniffing untuk mendapatkan akses terhadap Sister. Testing akan dilakukan secara manual dan disesuaikan dengan rencana pungujian yang telah dibuat pada tahap sebelumnya. Tahap ini akan membuktikan hasil penemuan celah dari tools yang

digunakan penulis terhadap Sister UNEJ apakah benar tidaknya terdapat celah pada sistem. Hasil dari penetration testing nantinya akan dilanjutkan dengan tahap ekploitasi.

4.3.5. Eksplotasi Celah

Pada tahap ini, penulis akan ekplotasi celah yang telah ditemukan pada tahap Penetration Testing. Penulis akan melakukan ekploitasi dari celah yang ditemukan seperti, merubah tampilan website, masuk sebagai admin, merubah dan menghapus informasi jika semua itu memungkinkan untuk dilakukan.

4.3.6. Analisis Hasil pengujian

Pada tahap Analisis Hasil Pengujian, penulis akan melakukan analisa terhadap serangkaian pengujian yang telah dilakukan. Dari hasil Pencarian Celah, Eksploitasi Celah, serta semua dampak yang disebabkan oleh celah keamanan. Dari celah yang ditemukan, penulis akan mengurutkan celah berdasarkan dampak dari celah dan ekploitasi celah berdasarkan hasil dari temuan *tools vulnerability scanner*. Kemudian penulis akan menyusun saran perbaikan terhadap celah keamanan yang telah ditemukan untuk dipertimbangkan oleh pihak UPT TI UNEJ untuk perbaikan terhadap sistem.

4.3.7. Clean up Sistem

Pada tahap *Clean Up* sistem, penulis akan melakukan pembersihan terhadap target pengujian. Penulis akan mengembalikan keadaan website seperti semula. Hal ini dilakukan agar sistem yang telah diretas kembali normal seperti

fungsi semula. *Clean up* dilakukan sejauh mana ekploitasi celah oleh penulis lakukan. Dari hasil ekploitasi, jika penulis menemukan informasi – informasi penting, penulis juga menghapus informasi tersebut dan menjaga kerahasiaan dari informasi tersebut agar tidak merugikan pihak Universitas Jember.

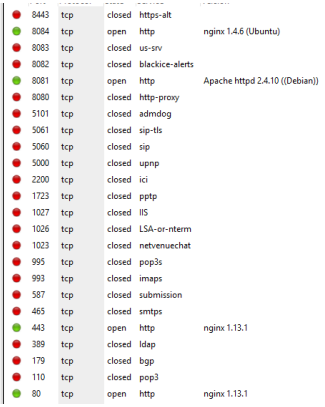
BAB V
IMPLEMENTASI

Pada bab 5 ini, penulis akan mengimplementasikan metodologi pengujian yang telah penulis tetapkan sebelumnya yaitu *Vulnerability Assesment & Penetration Testing.* Pada tahap implementasi penulis akan melaksanakan rencana pengujian yang telah disusun pada bab sebelumnya, Perancangan Evaluasi.

5.1. Pengintaian Sistem

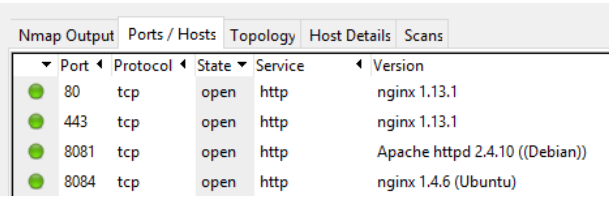
Pada tahap pengintaian sistem, akan dilakukan aktivitas pencarian informasi dasar target dan *melakukan port scanning* dengan menggunakan Nmap.

Pada Nmap, terdapat dua cara dalam melakukan *port scanning*. Pertama kita dapat melakukan pada *commad prompt* / *terminal* atau dengan menggunakan Zenmap. Zenmap adalah Nmap yang memiliki GUI. Zenmap mempermudah penguji untuk melakukan port scanning. Penguji hanya perlu mengetikkan target pengujian dan memilih *profile scan* yang diiginkan. Pada pengujian ini, penguji menggunakan *profile scan "slow comprehensive scan"* dimana Zenmap akan melakukan scan secara menyeluruh untuk mendapatkan informasi tentang *port*, *traceroute*, *topology,* dan informasi lainnya mengenai target pengujian. *Scanning* dengan menggunakan Zenmap akan dilakukan dua kali pada alamat sso.unej.ac.id dan sister.unej.ac.id.



8443	tcp	closed	https-alt	
8084	tcp	open	http	nginx 1.4.6 (Ubuntu)
8083	tcp	closed	us-srv	
8082	tcp	closed	blackice-alerts	
8081	tcp	open	http	Apache httpd 2.4.10 ((Debian))
8080	tcp	closed	http-proxy	
5101	tcp	closed	admdog	
5061	tcp	closed	sip-tls	
5060	tcp	closed	sip	
5000	tcp	closed	upnp	
2200	tcp	closed	ici	
1723	tcp	closed	pptp	
1027	tcp	closed	IIS	
1026	tcp	closed	LSA-or-nterm	
1023	tcp	closed	netvenuechat	
995	tcp	closed	pop3s	
993	tcp	closed	imaps	
587	tcp	closed	submission	
465	tcp	closed	smtps	
443	tcp	open	http	nginx 1.13.1
389	tcp	closed	ldap	
179	tcp	closed	bgp	
110	tcp	closed	pop3	
80	tcp	open	http	nginx 1.13.1

Gambar 5.1. port terbuka pada sso.unej.ac.id



Nmap Output | Ports / Hosts | Topology | Host Details | Scans

Port	Protocol	State	Service	Version
80	tcp	open	http	nginx 1.13.1
443	tcp	open	http	nginx 1.13.1
8081	tcp	open	http	Apache httpd 2.4.10 ((Debian))
8084	tcp	open	http	nginx 1.4.6 (Ubuntu)

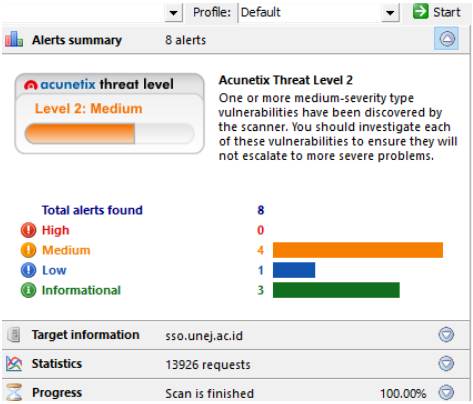
Gambar 5.2. Port terbuka pada sister.unej.ac.id

5.2. Pencarian Celah Keamanan

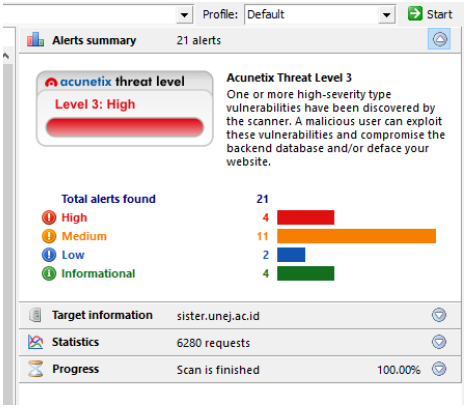
Pada tahap Pencarian Celah, akan dilaksanakan *Vulnerability Scanning* dengan menggunakan bantuan *tools software* yang telah ditentukan untuk pengujian. *Vulnerability Scanning* bertujuan untuk mencari celah keamanan pada target pengujian yang dapat disalah gunakan oleh pihak lain. Hasil dari pencarian celah keamanan akan digunakan untuk bahan Analisa dan *Penetration Testing* yang akan dilaksanakan pada tahap berikutnya.

5.2.1. Acunetix

Pada pengujian ini, penguji melakukan scanning sebanyak dua kali kepada sso.unej.ac.id dan sister.unej.ac.id. Pada pencarian celah dengan aplikasi Acunetix, penguji menggunakan profile default dimana pada profile ini, aplikasi melaksanakan semua tipe pencarian celah yang ada. Hasil pemindaian dapat dilihat pada gambar 5.3 dan gambar 5.4.



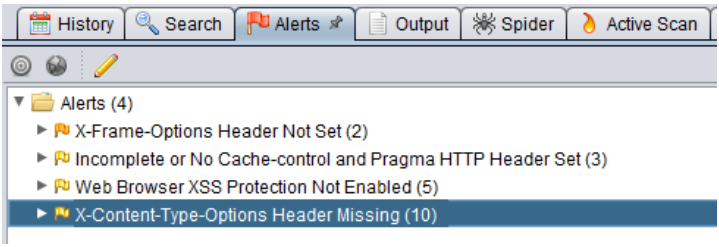
Gambar 5.3. Hasil temuan celah pada sso.unej.ac.id



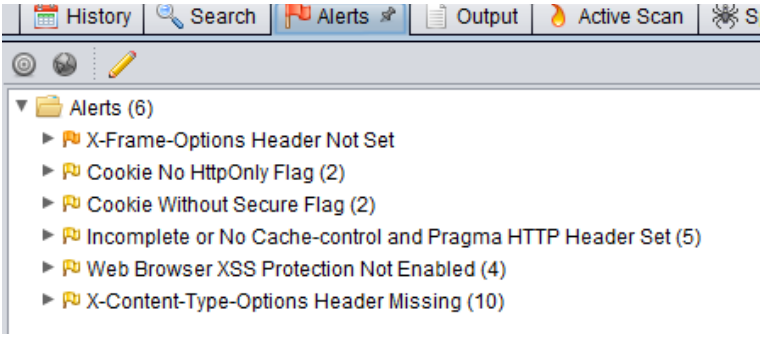
Gambar 5.4. Hasil temuan celah pada sister.unej.ac.id

5.2.2. OWASP ZAP

Selain menggunakan Acunetix, penguji juga menggunakan aplikasi OWASP ZAP. Pada pengujian ini, penguji juga melakukan pengujian sebanyak dua kali terhadap dua target yang berbeda. Penguji menggunakan profile Attack mode pada saat pemindaian. Hasil dari pemindaian dengan ZAP dapat dilihat pada gambar 5.5 dan gambar 5.6.



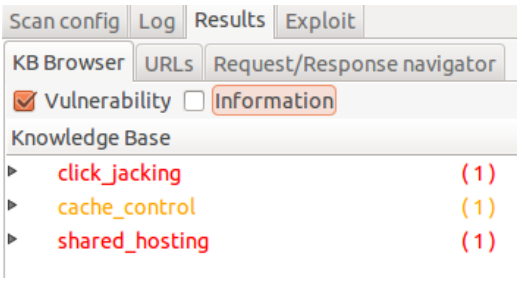
Gambar 5.5. Pencarian celah pada sso.unej.ac.id



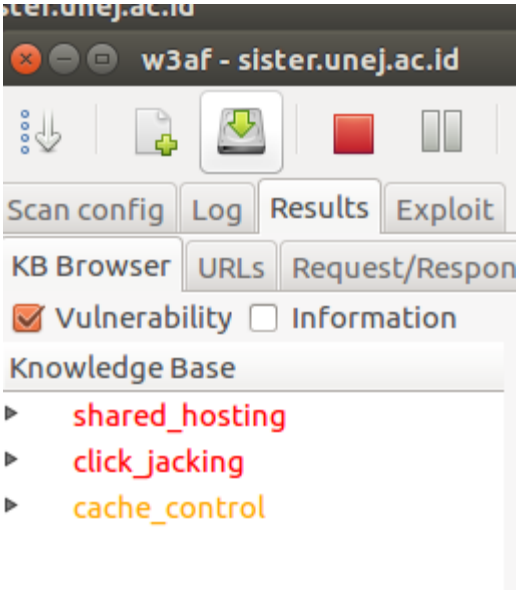
Gambar 5.6. Pencarian celah pada sister.unej.ac.id

5.2.3. W3af

Pada pengujian ini, penguji juga melakukan pengujian sebanyak dua kali terhadap dua target yang berbeda. Penguji menggunakan *profile custom*, dimana menggunakan *plugin audit, auth, crawl, grep*, dan *Inftrastructure*. Hasil dari pemindaian dengan w3af dapat dilihat pada gambar 5.7 dan gambar 5.8.



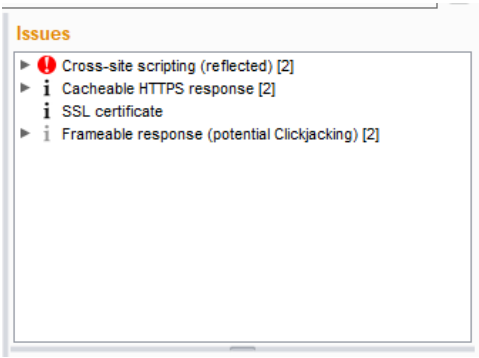
Gambar 5.7. Pencarian celah pada sso.unej.ac.id



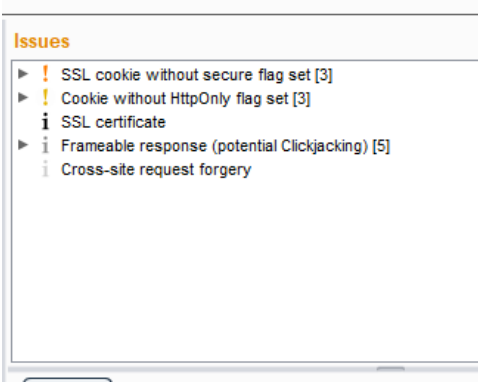
Gambar 5.8. Pencarian celah pada sister.unej.ac.id

5.2.4. Burp Suite

Pada penggunaan burp suite, penguji juga melakukan hal yang sama pada aplikasi sebelumnya, yaitu melakukan dua pengujian pada 2 alamat yang berbeda. Pada pengujian ini, penguji menggunakan beberapa fitur paa burp suite yaitu, proxy, spider, dan scanner. Hasil dari pencarian celah dengan aplikasi ini dipaparkan pada gambar 5.9 dan gambar 5.10.



Gambar 5.9. Pencarian celah pada sso.unej.ac.id

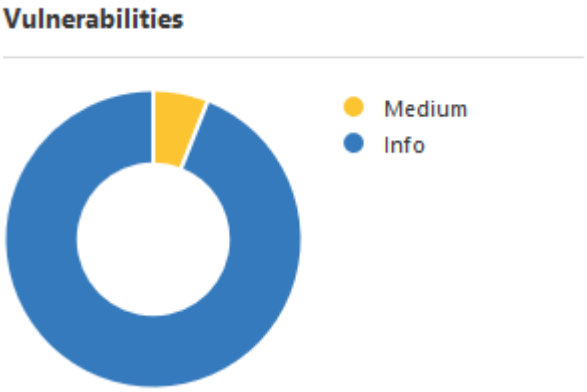


Gambar 5.10. Pencarian celah pada sister.unej.ac.id

5.2.5. Nessus

Pada pencarian celah yang terakhir, penguji menggunakan tools nessus. Namun pada pengujian ini, dilakukan pada satu IP dari sso.unej.ac.id. Hasil dari pencarian celah pada aplikasi ini

hanya ditemukan 1 celah yang memiliki rank *medium* dan sisa celah yang ditemukan memiliki rank *information*.



Gambar 5.11. Pencarian celah pada sso.unej.ac.id

5.3. Analisis dan Perencanaan Pengujian

Pada tahap Analisis dan Perencanaan Pengujian, penguji akan melaksanakan analisis dari dua tahap pengujian sebelumnya yaitu, pengintaian sistem dan pencarian celah. Analisa akan dilakukan untuk menentukan celah apa saja yang perlu diuji dan bagaimana mengujinya. Penjabaran Analisa celah keamanan yang ditemukan akan dijelaskan pada subbab berikutnya.

5.3.1. Celah pada sso.unej.ac.id

- Acunetix

1. Application Error Message
   Celah ini merupakan celah dimana suatu halaman dapat memunculkan sebuah pesan peringatan yang dapat

mengandung konten sensitif. Celah ini memiliki *ranking vulnerability medium*.

2. Cross Site Scripting (content sniffing)
   Celah ini mengindikasikan terdapat adanya form yang rentan terhadap Cross Site Scripting yang dipicu oleh content sniffing browser. Vulnerability ini memungkinkan penyerang atau hacker untuk mengirimkan code/script berbahaya kepada pengguna lain. Celah ini memiliki *ranking vulnerability medium.*
3. Clickjacking: X-Frame-Options Header Missing
   Clickjacking adalah celah dimana seorang hacker dapat readdress pada sebuah halaman yang terdapat website. Hal ini disebabkan tidak adanya X-Frame-Options dimana fungsinya adalah menunjukkan apakah browser diperbolehkan melakukan render suatu halaman di dalam frame atau iframe. Dengan adanya X-Frame-0ption, situs dapat mengetahui apakah konten didalam situs tersebut disematkan ke situs lain. Celah ini memiliki *ranking vulnerability low*.
4. Broken Links
   Pada sso.unej.ac.id terdapat sebuah link dimana tidak dapat diakses ataupun error saat diakses. Hal ini dapat diatasi dengan menghapus link ataupun membuat link tersebut dapat diakses. Celah ini *memiliki ranking vulnerability informational* dan tidak berbahaya terhadap website.
5. Possible Username or Password disclosure
   Terdapat file css pada website yang diduga mengandung username ataupun password user sso.unej.ac.id. hal ini

dapat dihindari dengan membuat file css tersebut tidak dapat diakses. Celah ini memiliki *ranking vulnerability informational*.

- OWASP ZAP

1. X-Frame-Option Header Not Set
   Celah ini mengindikasikan tidak adanya X-Frame-Option Header pada sso.unej.ac.id. hal ini dapat digunakan oleh seorang hacker untuk melakukan clickjacking. Celah ini memiliki ranking vulnerability medium.
2. Incomplete or No Cache-Control and Pragma HTTP Header Set
   Celah ini mengindikasikan tidak diaturnya Cache-Control dan Pragma HTTP header set pada sso.unej.ac.id. Hal ini dapat menyebabkan browser dapat menyimpan sebuah konten yang sensitif ataupun tidak dari website. Celah ini memiliki ranking vulnerability low.
3. Web Browser XSS Protection Not Enabled
   Celah ini mengindikasikan tidak diaktifkannya XSS *Protection* pada pengaturan htaccess ataupun file php pada sso.unej.ac.id sehingga terdapat kemungkinan terjadi XSS. Pada dasarnya kebanyakan browser telah memiliki fitur "XSS Filter" namun fitur ini tidak dapat aktif jika belum diaktifkan oleh pemilik situs. Celah ini memiliki ranking vulnerability low.
4. X-Content-Type-Options Header Missing
   Celah ini merupakan celah dimana "Anti-MIME-Sniffing header X-Content-Type-Options" tidak di set ke "nosniff". Namun browser baru cenderung sudah tidak dapat mengakses celah ini. Celah ini umumnya terjadi pada

browser versi lama seperti Internet Explorer 6 dan 7. Celah ini memiliki ranking vulnerability low.

- W3af
  1. Shared Hosting
     Celah ini ditemukan karena pada satu IP digunakan untuk banyak web. Hal ini dikarenakan sso.unej.ac.id menggunakan single-sign-on dimana user menggunakan satu username untuk banyak web aplikasi yang ada pada Universitas Jember.
  2. Clickjacking
     Clickjacking adalah celah dimana seorang hacker dapat readdress pada sebuah halaman yang terdapat website. Hal ini disebabkan tidak adanya X-Frame-Options dimana fungsinya adalah menunjukkan apakah browser diperbolehkan melakukan render suatu halaman di dalam frame atau iframe. Dengan adanya X-Frame-0ption, situs dapat mengetahui apakah konten didalam situs tersebut disematkan ke situs lain. Celah ini memiliki *ranking vulnerability low.*
  3. Cache Control
     Celah ini mengindikasikan tidak diaturnya Cache-Control dan Pragma HTTP header set pada sso.unej.ac.id. Hal ini dapat menyebabkan browser dapat menyimpan sebuah konten yang sensitif ataupun tidak dari website. Celah ini memiliki *ranking vulnerability low*.
- Burp Suite
  1. Cross Site Scripting (reflected)

Celah ini mengindikasikan bahwa terdapat halaman yang rentan terhadap serangan *Cross Site Scripting* (XSS). *Cross site scripting* adalah kerentanan yang memungkinkan penyerang untuk mengirim kode berbahaya (biasanya berupa Javascript) ke pengguna lain. Karena browser tidak dapat mengetahui apakah script tersebut harus dipercaya atau tidak, maka script tersebut akan dieksekusi script dalam konteks pengguna yang memungkinkan penyerang mengakses cookie atau token sesi yang disimpan oleh browser. Celah ini memiliki ranking celah

2. Cacheable HTTPS Response
   Celah ini mengindikasikan terdapat file yang dapat tersimpan pada browser. File yang tersimpan tersebut dikhawatirkan mengandung informasi sensitive yang dapat disalahgunakan.
3. SSL certificate
   Informasi ini mengindikasikan server sister Universitas Jember menggunakan "trusted SSL certificate".
4. Frameable Respone (potential Clickjacking)
   Clickjacking adalah celah dimana seorang hacker dapat readdress pada sebuah halaman yang terdapat website. Hal ini disebabkan tidak adanya X-Frame-Options dimana fungsinya adalah menunjukkan apakah browser diperbolehkan melakukan render suatu halaman di dalam frame atau iframe. Dengan adanya X-Frame-0ption, situs dapat mengetahui apakah konten didalam situs tersebut disematkan ke situs lain. Celah ini memiliki *ranking vulnerability low.*

- Nessus

1. Web Application Potentially Vulnerable to Clickjacking
   Clickjacking adalah celah dimana seorang hacker dapat readdress pada sebuah halaman yang terdapat website. Hal ini disebabkan tidak adanya X-Frame-Options dimana fungsinya adalah menunjukkan apakah browser diperbolehkan melakukan render suatu halaman di dalam frame atau iframe. Dengan adanya X-Frame-0ption, situs dapat mengetahui apakah konten didalam situs tersebut disematkan ke situs lain. Celah ini memiliki *ranking vulnerability medium*
2. Web Application Cookies Not Marked Secure
   Informasi ini mengindikasikan bahwa terdapat cookie yang tidak diatur dengan *secure flag*. Hal ini dapat menyebabkan cookie dapat diakses melalui koneksi yang tidak terenkripsi. Celah ini bersifat information.
3. External URLs
   Informasi ini mengindikasikan ketika melakukan akses terhadap website didalam single-sign-on tidak melalui sso.unej.ac.id maka akan otomatis akan redirect ke halaman sso.unej.ac.id.
4. Web Application Sitemap
   Informasi ini mengindikasikan terdapat konten yang dapat diakses dari webserver. Konten tersebut dapat digunakan untuk mengumpulkan informasi mengenai target (sso.unej.ac.id)
5. Web Server No 404 Error Code Check

Informasi ini mengindikasikan web server tidak memiliki error code check ketika mengakses file atau halaman yang tidak terdapat pada webserver.

5.3.2. Celah pada sister.unej.ac.id

- Acunetix

1. Cross Site Scripting (verified)
   Celah ini mengindikasikan bahwa terdapat halaman yang rentan terhadap serangan *Cross Site Scripting* (XSS). *Cross site scripting* adalah kerentanan yang memungkinkan penyerang untuk mengirim kode berbahaya (biasanya berupa Javascript) ke pengguna lain. Karena browser tidak dapat mengetahui apakah script tersebut harus dipercaya atau tidak, maka script tersebut akan dieksekusi script dalam konteks pengguna yang memungkinkan penyerang mengakses cookie atau token sesi yang disimpan oleh browser. Celah ini memiliki *ranking vulnerability high*.
2. Application Error Message
   Celah ini merupakan celah dimana suatu halaman dapat memunculkan sebuah pesan peringatan yang dapat mengandung konten sensitif. Celah ini memiliki *ranking vulnerability medium*.
3. HTML Form without CSRF Protection
   Celah ini mengindikasikan bahwa pada situs terdapat form yang tidak dilindungi oleh CSRF Protection. Tidak adanya perlindunagan CSRF, dapat mengakibatkan server mendapatkan *unauthorized command* dari pengguna yang

dipercaya oleh server atau biasa disebut *session riding*. Celah ini memiliki *ranking vulnerability medium*.

4. Vulnerable Javascript Library
   Celah ini mengindikasikan bahwa web menggunakan *outdated javascript library.* penggunaan library ini dimuat secara *inline* atau *transitively* melalui *third-party code/widget* yang cenderung memiliki kerentanan lebih tinggi dibandingkan dengan JS library yang dimuat langsung dari panggilan skrip pada situs. Celah ini memiliki *ranking vulnerability medium.*
5. Clickjacking: X-Frame-Options Header Missing
   Clickjacking adalah celah dimana seorang hacker dapat readdress pada sebuah halaman yang terdapat website. Hal ini disebabkan tidak adanya X-Frame-Options dimana fungsinya adalah menunjukkan apakah browser diperbolehkan melakukan render suatu halaman di dalam frame atau iframe. Dengan adanya X-Frame-0ption, situs dapat mengetahui apakah konten didalam situs tersebut disematkan ke situs lain. Celah ini memiliki *ranking vulnerability low.*
6. Cookie Without Httponly Flag Set
   Celah ini mengindikasikan bahwa terdapat cookie yang tidak tidak di set *HTTPOnly Flag*-nya. Hal ini dapat membuat cookie diakses oleh pihak pengguna yang seharusnya hanya dapat diakses oleh server. Celah ini memiliki *ranking vulnerability low*
7. Email Address Found
   Celah ini menginidikasikan terdapat halaman web yang menampilkan satu atau lebih email. Hal ini ditakutkan akan

digunakan oleh spam-bots untuk melakukan hal – hal yang tidak diinginkan oleh pemiliki email tersebut. Celah ini memiliki *ranking vulnerability informational.*

8. Password Type Input with auto-completed enabled
   Celah ini mengindikasikan bahwa terdapat fitur *auto-completed* pada browser yang digunakan user. Hal ini berbahaya jika terdapat hacker yang mengguanakan akses lokal yang dapat menggunakan hal tersebut untuk mendapatkan password dari browser cache. Celah ini memiliki *ranking vulnerability informational*

- OWASP ZAP

1. X-Frame-Option Header Missing
   Celah ini mengindikasikan tidak adanya X-Frame-Option Header pada sso.unej.ac.id. hal ini dapat digunakan oleh seorang hacker untuk melakukan clickjacking. Celah ini memiliki *ranking vulnerability medium.*
2. Cookie No HttpOnly Flag
   Celah ini mengindikasikan bahwa terdapat cookie yang tidak tidak di set *HTTPOnly Flag*-nya. Hal ini dapat membuat cookie diakses oleh pihak pengguna yang seharusnya hanya dapat diakses oleh server. Celah ini memiliki *ranking vulnerability low.*
3. Cookie Without Secure Flag
   Celah ini mengindikasikan bahwa terdapat cookie yang tidak diatur dengan *secure flag.* Hal ini dapat menyebabkan cookie dapat diakses melalui koneksi yang tidak terenkripsi. Cookie tersebut dapat mengandung konten/informasi sensitif yang bisa disalahgunakan. Celah ini memiliki *ranking vulnerability low.*

4. Incomplete or No Cache-Control and Pragma HTTP Header Set
   Celah ini mengindikasikan tidak diaturnya Cache-Control dan Pragma HTTP header set pada sso.unej.ac.id. Hal ini dapat menyebabkan browser dapat menyimpan sebuah konten yang sensitif ataupun tidak dari website. Celah ini memiliki *ranking vulnerability low*.
5. Web Browser XSS Protection Not Enabled
   Celah ini mengindikasikan tidak diaktifkannya XSS Protection pada pengaturan htaccess ataupun file php pada sso.unej.ac.id sehingga terdapat kemungkinan terjadi XSS. Pada dasarnya kebanyakan browser telah memiliki fitur "XSS Filter" namun fitur ini tidak dapat aktif jika belum diaktifkan oleh pemilik situs. Celah ini memiliki *ranking vulnerability low*.
6. X-Content-Type-Options Header Missing
   Celah ini merupakan celah dimana Anti-MIME-Sniffing header X-Content-Type-Options tidak di set ke "nosniff". Namun browser baru cenderung sudah tidak dapat mengakses celah ini. Celah ini umumnya terjadi pada browser versi lama seperti Internet Explorer 6 dan 7. Celah ini memiliki ranking vulnerability low.

- W3af

1. Shared Hosting
   Celah ini ditemukan karena pada satu IP digunakan untuk banyak web. Hal ini dikarenakan sso.unej.ac.id menggunakan single-sign-on dimana user menggunakan satu username untuk banyak web aplikasi yang ada pada Universitas Jember.

2. Clickjacking
   Clickjacking adalah celah dimana seorang hacker dapat readdress pada sebuah halaman yang terdapat website. Hal ini disebabkan tidak adanya X-Frame-Options dimana fungsinya adalah menunjukkan apakah browser diperbolehkan melakukan render suatu halaman di dalam frame atau iframe. Dengan adanya X-Frame-0ption, situs dapat mengetahui apakah konten didalam situs tersebut disematkan ke situs lain. Celah ini memiliki *ranking vulnerability low*.
3. Cache Control
   Celah ini mengindikasikan tidak diaturnya Cache-Control dan Pragma HTTP header set pada sso.unej.ac.id. Hal ini dapat menyebabkan browser dapat menyimpan sebuah konten yang sensitif ataupun tidak dari website. Celah ini memiliki *ranking vulnerability low*.

- Burp suite

1. SSL cookie without secure flag set
   Celah ini mengindikasikan bahwa terdapat cookie yang tidak diatur dengan *secure flag*. Hal ini dapat menyebabkan cookie dapat diakses melalui koneksi yang tidak terenkripsi. Cookie tersebut dapat mengandung konten/informasi sensitif yang bisa disalahgunakan
2. Cookie without httponly flag set
   Celah ini mengindikasikan bahwa terdapat cookie yang tidak tidak di set *HTTPOnly Flag*-nya. Hal ini dapat membuat cookie diakses oleh pihak pengguna yang seharusnya hanya dapat diakses oleh server.
3. SSL certificate

Informasi ini mengindikasikan server sister Universitas Jember menggunakan “trusted SSL certificate”.

4. Frameable Response (Potentially Clickjacking)
   Clickjacking adalah celah dimana seorang hacker dapat readdress pada sebuah halaman yang terdapat website. Hal ini disebabkan tidak adanya X-Frame-Options dimana fungsinya adalah menunjukkan apakah browser diperbolehkan melakukan render suatu halaman di dalam frame atau iframe. Dengan adanya X-Frame-0ption, situs dapat mengetahui apakah konten didalam situs tersebut disematkan ke situs lain.
5. Cross-site Request Forgery
   Celah ini mengindikasikan bahwa pada situs terdapat form yang tidak dilindungi oleh CSRF Protection. Tidak adanya perlindunagan CSRF, dapat mengakibatkan server mendapatkan *unauthorized command* dari pengguna yang dipercaya oleh server atau biasa disebut *session riding*. Celah ini memiliki *ranking vulnerability medium*.

5.3.3. Daftar Celah yang Diuji

- sso.unej.ac.id

Table 5.1.Celah sso.unej.ac.id

No	Nama Celah	Level	Status	Keterangan
1	Application Error Message	Medium	Diuji	

No	Nama Celah	Level	Status	Keterangan
2	Cross Site Scripting (content sniffing)	Medium	Diuji	
3	X-Frame-Option Header Not Set	Medium	Diuji	
4	Incomplete or No Cache-Control and Pragma HTTP Header Set	Low	Diuji	
5	Web Browser XSS Protection Not Enabled	Low	Tidak diuji	Celah ini ada karena tidak terdapat script/code untuk mengaktifkan XSS protection. XSS sendiri nantinya akan diuji.
6	X-Content-Type-Options	Low	Tidak diuji	Celah hanya dapat terjadi pada web browser versi lama seperti Internet Explore 6 dan 7.

No	Nama Celah	Level	Status	Keterangan
	Header Missing			Dengan asumsi tidak ada lagi yang menggunakan browser tersebut.
7	Possible Username or Password disclosure	Information	Diuji	
8	Broken Links	Information	Tidak diuji	Links tersebut ketika diakses melalui website, secara otomatis web akan me-redirect link menuju halaman utama.
9	Shared Hosting	Information	Tidak diuji	Bersifat informasi dan tidak memiliki dampak bagi sistem.
10	External URLs	Information	Tidak diuji	Bersifat informasi dan tidak memiliki dampak bagi sistem.

- sister.unej.ac.id

Table 5.2. celah sister.unej.ac.id

No	Nama Celah	Level	Status	Keterangan
1	Cross Site Scripting (verified)	High	Diuji	
2	Application Error Message	Medium	Diuji	
3	HTML Form without CSRF Protection	Medium	Diuji	
4	Vulnerable Javascript Library	Medium	Tidak diuji	Bersifat informasi bahwa javascript yang digunakan telah *out-of-date*
5	X-Frame-Option Header Not Set	Medium	Diuji	
6	Cookie Without	Low	Tidak Diuji	

No	Nama Celah	Level	Status	Keterangan
	Httponly Flag Set			
7	Cookie Without Secure Flag	Low	Tidak Diuji	
8	Incomplete or No Cache-Control and Pragma HTTP Header Set	Low	Diuji	
9	Web Browser XSS Protection Not Enabled	low	Tidak diuji	Celah ini ada karena tidak terdapat script/code untuk mengaktifkan XSS protection. XSS sendiri nantinya akan diuji.
10	X-Content-Type-	Low	Tidak diuji	Celah hanya dapat terjadi pada

No	Nama Celah	Level	Status	Keterangan
	Options Header Missing			web browser versi lama seperti Internet Explore 6 dan 7. Dengan asumsi tidak ada lagi yang menggunakan browser tersebut.
11	Email Address Found	Information	Diuji	Email yang muncul tersebut berasal dari Jquery yang bukan milik pihak Universitas Jember.
12	Password Type Input with auto-completed enabled	Information	Tidak diuji	Celah ini terdapat pada browser yang menyimpan username dan password dari user.
13	SSL certificate	Information	Tidak diuji	Bersifat informasi dan tidak

No	Nama Celah	Level	Status	Keterangan
				berdampak pada sistem.

Sebagai pembanding atas temuan – temuan celah yang didapat dengan bantuan aplikasi, penulis melakukan interview terhadap kepala UPT TI Universitas Jember terkait serangan – serangan apa saja yang pernah dialami oleh Sister Universitas Jember.

Table 5.3. tabel history serangan sister unej

No	Serangan	Status	Dampak	Kronologi
1	SQL Injection	Telah diperbaiki	Didapatnya hak akses admin. Merubah nilai mahasiswa.	Hacker melakukan sql injection terhadap sistem dan mendapatkan hak akses admin. Kemudian hacker menggunakan hak akses tersebut untuk merubah informasi yang terdapat pada sister universitas jember. Salah satunya adalah nilai mahasiswa.

5.4. Penetration Testing

Setelah melakukan analisis celah yang dilakukan pada sub bab sebelumnya, didapatkan hasil celah yang dapat dilakukan *penetration testing* yang dijelaskan pada table 5.1 dan table 5.2.

- Sso.unej.ac.id
    - *Application Error Message*
    - *Cross Site Scripting (content sniffing)*
    - *X-Frame-Option Header Not Set*
    - *Possible Username or Password Disclosure*
    - *Incomplete or No Cache-Control and Pragma HTTP Header Set*
- Sister.unej.ac.id
    - *Cross Site Scripting (verified)*
    - *Application Error Message*
    - *HTML Form without CSRF Protection*
    - *X-Frame-Option Header Not Set*
    - *Incomplete or No Cache-Control and Pragma HTTP Header Set*

Untuk hasil dari pengujian pada celah yang telah ditentukan, akan dijelaskan pada Bab VI pada sub bab 6.4.

5.5. Eksploitasi Celah

Pada tahap Penetration testing tidak didapat celah yang dapat memberikan penguji untuk akses masuk ke dalam sistem, sehingga penguji melakukan phising. Hasil dari phising tersebut didapatkan user milik salah satu mahasiswa di Universitas Jember.

5.6. Analisis Hasil Pengujian

Pada tahap analis hasil pengujian dijelaskan dengan detail pada bab 6 serta rekomendasi yang dapat dijadikan sebagai bahan pertimbangan terhadap Sister Universitas Jember.

5.7. Clean Up Sistem

Pada tahap Clean Up sistem(pembersihan) penguji merubah kembali semua informasi yang sebelumnya diubah pada saat ekploitasi celah.

(Halaman ini sengaja dikosongkan)

BAB VI
HASIL DAN PEMBAHASAN

Pada bab ini, dipaparkan hasil dari pengujian terhadap Sister Universitas Jember yang telah dilakukan oleh penulis. Pemaparan hasil penelitian dipaparkan sesuai dengan tahapan pada bab IV dan bab V.

6.1. Pengintaian Sistem

Pada pengintaian sistem telah dilakukan pengujian dengan bantuan tools Nmap. Hasil dari Port Scanning yang dilakukan Nmap dapat dilihat pada gambar 5.1 dan gambar 5.2. Dari hasil tersebut ditemukan beberapa port yang terbuka yang akan dijelaskan pada table 6.1 dan table 6.2.

Table 6.1. Port sso.unej.ac.id

Port yang terbuka	Protocol	Deskripsi
80	TCP	Port ini digunakan untuk Hypertext Transfer Protocol (HTTP). Dengan kata lain, port ini dibuka agar website Sister UNEJ dapat diakses.

Port yang terbuka	Protocol	Deskripsi
443	TCP	Port ini digunakan untuk Hypertext Transfer Protocol dengan tambahan SSL (HTTPS). Dengan kata lain, port ini dibuka agar website Sister UNEJ dapat diakses.
8081	TCP	Port ini digunakan untuk utilistor server dan juga Apache httpd 2.4.10
8084	TCP	Port ini digunakan TCP Tunneling port untuk Audio/Video. Port ini juga digunakan nginx 1.4.6.

Table 6.2. port sister.unej.ac.id

Port yang terbuka	Protocol	Deskripsi
80	TCP	Port ini digunakan untuk Hypertext Transfer Protocol (HTTP). Dengan kata lain, port ini dibuka agar website Sister UNEJ dapat diakses.
443	TCP	Port ini digunakan untuk Hypertext Transfer Protocol dengan tambahan SSL (HTTPS). Dengan kata lain, port ini dibuka agar website Sister UNEJ dapat diakses.
8081	TCP	Port ini digunakan untuk utilistor server dan juga

Port yang terbuka	Protocol	Deskripsi
		Apache httpd 2.4.10
8084	TCP	Port ini digunakan TCP Tunneling port untuk Audio/Video. Port ini juga digunakan nginx 1.4.6.

6.2. Pencarian Celah

Pada pencarian celah, penguji menggunakan 2 aplikasi *vulnerability scanner* yaitu acunetix dan owasp zap. Hasil dari pencarian celah akan dibahas pada sub bab berikut.

6.2.1. Hasil Pencarian Celah Acunetix

Pencarian celah dengan menggunakan aplikasi Acunetix menghasilkan beberapa temuan celah yang terdapat pada 2 alamat website yang berbeda yang akan dijelaskan pada table 6.3 dan table 6.4.

Table 6.3. celah pada sso.unej.ac.id

No	Celah Keamanan	Rank Vulnerability	Deskripsi	Dampak
1	Application error Message	Medium	Pada halaman cas/login dapat memunculkan suatu pesan	Dapat memunculkan informasi sensitive ketika

No	Celah Keamanan	Rank Vulnerability	Deskripsi	Dampak
			peringatan karena adanya input yang tidak dapat ditangani	pesan error muncul.
2	Cross Site Scripting (Content Sniffing)	Medium	XSS adalah celah dimana penyerang dapat menyisipkan script yang dapat merubah tampilan web	Dapat merubah tampilan web, menyisipkan link ke site lain.
3	Clickjacking: X-Frame-options header missing	Low	Clickjacking adalah celah dimana seorang hacker dapat readdress pada sebuah button yang terdapat website. Hal ini disebabkan tidak adanya X-Frame-Options dimana fungsinya adalah menunjukkan apakah browser diperbolehkan	Dapat digunakan untuk tools social engineering (Clickjacking)

No	Celah Keamanan	Rank Vulnerability	Deskripsi	Dampak
			melakukan render suatu halaman di dalam frame atau iframe.	
4	Broken Links	Informational	Celah ini mengindikasikan terdapat file yang tidak dapat diakses	-
5	Possible Username or password disclosure	Informational	Celah ini mengindikasikan bahwa terdapat file yang mungkin mengandung username atau password	Dapat mengandung konten sensitif yang disalahgunakan.

Table 6.4. celah pada sister.unej.ac.id

No	Celah Keamanan	Rank Vulnerability	Deskripsi	Dampak
1	Cross Site Scripting (verified)	High	XSS adalah celah dimana penyerang dapat menyisipkan script yang dapat merubah tampilan web	Dapat merubah tampilan web, menyisipkan link ke site lain
2	Application error message	Medium	Pada halaman cas/login dapat memunculkan suatu pesan peringatan, karena adanya input yang tidak dapat ditangani	Dapat memunculkan informasi sensitif.
3	HTML form without CSRF protection	Medium	CSRF adalah serangan dimana hacker menggunakan hak/akses user tanpa dikehendakinya	Dapat terjadinya manipulasi data, perubahan data seperti password.

No	Celah Keamanan	Rank Vulnerability	Deskripsi	Dampak
4.	Vulnerable Javascript Library			
4	Clickjacking: X-Frame-options header missing	Low	Clickjacking adalah celah dimana seorang hacker dapat readdress pada sebuah button yang terdapat website. Hal ini disebabkan tidak adanya X-Frame-Options dimana fungsinya adalah menunjukkan apakah browser diperbolehkan menampilkan suatu halaman di dalam frame atau iframe.	Dapat digunakan untuk tools social engineering (Clickjacking)

No	Celah Keamanan	Rank Vulnerability	Deskripsi	Dampak
5	Email address found	Informational	Celah ini mengindikasikan terdapat file yang mengandung alamat email	Penyalahgunaan alamat email seperti spam.
6	Password type input with auto-completed enabled	Informational	Celah ini mengindikasikan bahwa web menginjinkan browser menyimpan password dan username.	Informasi email dan password dapat disalah gunakan oleh pihak lain.

6.2.2. Hasil Pencarian Celah OWASP ZAP

Pencarian celah dengan menggunakan aplikasi OWASP ZAP menghasilkan beberapa temuan celah yang terdapat pada 2 alamat website yang berbeda yang akan dijelaskan pada table 6.5 dan table 6.6.

Table 6.5. celah pada sso.unej.ac.id

No	Celah Keamanan	Rank Vulnerability	Deskripsi	Dampak
1	X-Frame-Options	Medium	Clickjacking adalah celah	Dapat digunakan

No	Celah Keamanan	Rank Vulnerability	Deskripsi	Dampak
	Header not set		dimana seorang hacker dapat readdress pada sebuah tampilan yang terdapat di web. Hal ini disebabkan tidak adanya X-Frame-Options dimana fungsinya adalah menunjukkan apakah browser diperbolehkan melakukan render suatu halaman di dalam frame atau iframe.	untuk tools social engineering (Clickjacking)
2	Incomplete or No Cache-control and Pragma HTTP Header Set	Low	Celah ini mengindikasikan tidak diaturnya Cache-Control dan Pragma HTTP header set pada sso.unej.ac.id.	Hal ini dapat menyebabkan browser dapat menyimpan sebuah konten yang sensitif ataupun tidak dari website

No	Celah Keamanan	Rank Vulnerability	Deskripsi	Dampak
3	Web Browser XSS Protection Not Enabled	Low	Celah ini mengindikasikan tidak diaktifkannya XSS *Protection* pada pengaturan htaccess ataupun file php pada web. Pada dasarnya kebanyakan browser telah memiliki fitur "XSS Filter" namun fitur ini tidak dapat aktif jika belum diaktifkan oleh pemilik web.	Rentan akan serangan XSS
4	X-Content-Type-Options Header Missing	Low	Celah ini merupakan celah dimana "Anti-MIME-Sniffing header X-Content-Type-Options" tidak di set ke "nosniff". Namun browser baru cenderung sudah	Rentan untuk MIME-type sniffing

No	Celah Keamanan	Rank Vulnerability	Deskripsi	Dampak
			tidak dapat mengakses celah ini. Celah ini umumnya terjadi pada browser versi lama seperti Internet Explorer 6 dan 7.	

Table 6.6. celah pada sister.unej.ac.id

No	Celah Keamanan	Rank Vulnerability	Deskripsi	Dampak
1	X-Frame-Options Header not set	Medium	Clickjacking adalah celah dimana seorang hacker dapat readdress pada sebuah tampilan yang terdapat di web. Hal ini disebabkan tidak adanya X-Frame-Options dimana fungsinya adalah menunjukkan	Dapat digunakan untuk tools social engineering (Clickjacking)

No	Celah Keamanan	Rank Vulnerability	Deskripsi	Dampak
			apakah browser diperbolehkan melakukan render suatu halaman di dalam frame atau iframe.	
2	Cookie No HttpOnly Flag	Low	Celah ini mengindikasikan bahwa cookies rentan akan diakses dan dikirim ke situs lain.	Session hijacking
3	Cookie Without Secure Flag	low	Celah ini mengindikasikan bahwa cookies dapat diakses melalui konek yang tidak terenkripsi. Namun UNEJ telah menggunakan https.	Dikhawatirkan cookie mengandung konten sensitive.

No	Celah Keamanan	Rank Vulnerability	Deskripsi	Dampak
4	Incomplete or No Cache-control and Pragma HTTP Header Set	Low	Celah ini mengindikasikan tidak diaturnya Cache-Control dan Pragma HTTP header set pada sister.unej.ac.id.	Hal ini dapat menyebabkan browser dapat menyimpan sebuah konten yang sensitif ataupun tidak dari website
5	Web Browser XSS Protection Not Enabled	Low	Celah ini mengindikasikan tidak diaktifkannya XSS *Protection* pada pengaturan htaccess ataupun file php pada web. Pada dasarnya kebanyakan browser telah memiliki fitur "XSS Filter" namun fitur ini tidak dapat aktif jika belum diaktifkan oleh pemilik web.	Rentan akan serangan XSS

No	Celah Keamanan	Rank Vulnerability	Deskripsi	Dampak
6	X-Content-Type-Options Header Missing	Low	Celah ini merupakan celah dimana "Anti-MIME-Sniffing header X-Content-Type-Options" tidak di set ke "nosniff". Namun browser baru cenderung sudah tidak dapat mengakses celah ini. Celah ini umumnya terjadi pada browser versi lama seperti Internet Explorer 6 dan 7.	Rentan untuk MIME-type sniffing

6.2.3. Hasil Pencarian Celah W3af

Pencarian celah dengan menggunakan aplikasi w3af menghasilkan beberapa temuan celah yang terdapat pada 2 alamat website yang berbeda yang akan dijelaskan pada table 6.7 dan table 6.8.

Table 6.7. celah pada sso.unej.ac.id

No	Celah Keamanan	Rank Vulnerability	Deskripsi	Dampak
1	Shared Hosting	information	Web aplikasi menggunakan shared hosting yang digunakan untuk beberapa domain secara bersamaan	-
2	Clickjacking	low	Clickjacking adalah celah dimana seorang hacker dapat readdress pada sebuah tampilan yang terdapat di web. Hal ini disebabkan tidak adanya X-Frame-Options dimana fungsinya adalah menunjukkan apakah browser diperbolehkan melakukan render suatu halaman di	Dapat digunakan untuk tools social engineering (Clickjacking)

No	Celah Keamanan	Rank Vulnerability	Deskripsi	Dampak
3	Cache Control		Celah ini mengindikasikan tidak diaturnya Cache-Control dan Pragma HTTP header set pada sso.unej.ac.id.	Hal ini dapat menyebabkan browser dapat menyimpan sebuah konten yang sensitif ataupun tidak dari website

Table 6.8. celah pada sister.unej.ac.id

No	Celah Keamanan	Rank Vulnerability	Deskripsi	Dampak
2	Clickjacking	low	Clickjacking adalah celah dimana seorang hacker dapat readdress pada sebuah tampilan yang terdapat di web. Hal ini disebabkan tidak adanya X-Frame-Options dimana fungsinya adalah menunjukkan	Dapat digunakan untuk tools social engineering (Clickjacking)

No	Celah Keamanan	Rank Vulnerability	Deskripsi	Dampak
			apakah browser diperbolehkan melakukan render suatu halaman di	
3	Cache Control		Celah ini mengindikasikan tidak diaturnya Cache-Control dan Pragma HTTP header set pada sso.unej.ac.id.	Hal ini dapat menyebabkan browser dapat menyimpan sebuah konten yang sensitif ataupun tidak dari website

6.2.4. Hasil Pencarian Celah Burp Suite

Pencarian celah dengan menggunakan aplikasi Burp Suite menghasilkan beberapa temuan celah yang terdapat pada 2 alamat website yang berbeda yang akan dijelaskan pada table 6.9 dan table 6.10.

Table 6.9. Celah pada sso.unej.ac.id

No	Celah Keamanan	Rank Vulnerability	Deskripsi	Dampak
1	Cross Site Scripting (Reflected)	Information	XSS adalah celah dimana penyerang dapat menyisipkan script yang dapat merubah tampilan web terhadap XSS pada	Muncul error message
2	SSL Certificate	Information	Mengindikasikan server telah menggunakan sertifikat SSL terpercaya	-
3	Frameable Response (Potentially Clickjacking)	Information	Clickjacking adalah celah dimana seorang hacker dapat readdress pada sebuah tampilan yang terdapat di web. Hal ini disebabkan tidak adanya X-Frame-Options	Dapat digunakan untuk tools social engineering (Clickjacking)

No	Celah Keamanan	Rank Vulnerability	Deskripsi	Dampak
			dimana fungsinya adalah menunjukkan apakah browser diperbolehkan melakukan render suatu halaman di dalam frame atau iframe.	

Table 6.10. celah pada sister.unej.ac.id

No	Celah Keamanan	Rank Vulnerability	Deskripsi	Dampak
1	SSL cookie without secure flag set	Medium	Celah ini mengindikasikan bahwa cookies rentan akan diakses dan dikirim ke situs lain.	Session hijacking
2	Cookie without	Low	Celah ini mengindikasikan bahwa cookies dapat diakses	Dikhawatirkan cookie mengandung konten

No	Celah Keamanan	Rank Vulnerability	Deskripsi	Dampak
	httponly flag set		melalui konek yang tidak terenkripsi. Namun UNEJ telah menggunakan https.	sensitive seperti username dan password.
	SSL Certificate	Information	Mengindikasikan server telah menggunakan sertifikat SSL terpercaya	-
4	Frameable Response (Potentially Clickjacking)	Information	Clickjacking adalah celah dimana seorang hacker dapat readdress pada sebuah tampilan yang terdapat di web. Hal ini disebabkan tidak adanya X-Frame-Options dimana fungsinya adalah menunjukkan apakah browser	Dapat digunakan untuk tools social engineering (Clickjacking)

No	Celah Keamanan	Rank Vulnerability	Deskripsi	Dampak
			diperbolehkan melakukan render suatu halaman di dalam frame atau iframe.	

6.2.5. Hasil Pencarian Celah Nessus

Pencarian celah dengan menggunakan aplikasi Nessus menghasilkan beberapa temuan celah yang akan dijelaskan pada table 6.11.

Table 6.11. celah pada sso.unej.ac.id

No	Celah Keamanan	Rank Vulnerability	Deskripsi	Dampak
1	Web application Potentially Vulnerable to Clickjacking	Medium	Clickjacking adalah celah dimana seorang hacker dapat readdress pada sebuah tampilan yang terdapat di web. Hal ini disebabkan tidak adanya X-Frame-	Dapat digunakan untuk tools social engineering (Clickjacking)

No	Celah Keamanan	Rank Vulnerability	Deskripsi	Dampak
			Options dimana fungsinya adalah menunjukkan apakah browser diperbolehkan melakukan render suatu halaman di dalam frame atau iframe.	
2	Web Application Cookies Not Marked Secure	Information	Celah ini mengindikasikan bahwa cookies dapat diakses melalui konek yang tidak terenkripsi. Namun UNEJ telah menggunakan https.	Dikhawatirkan cookie mengandung konten sensitive.
3	External URLs	Information	Infomarsi ini mengindikasi setiap domain yang terdapat pada sso.unej.ac.id tidak dapat	-

No	Celah Keamanan	Rank Vulnerability	Deskripsi	Dampak
			diakses sebelum login.	
4	Web Application Sitemap	Information	Informasi ini mengindikasikan terdapat konten yang dapat diakses dari webserver. Konten tersebut dapat digunakan untuk mengumpulkan informasi mengenai target (sso.unej.ac.id)	-

6.3. Analisis dan Perencanaan Pengujian

Hasil dari analisis dan perencaan pengujian telah dijelaskan pada bab V dimana didapat beberapa celah yang akan diuji yaitu:

- Sso.unej.ac.id
  - *Application Error Message*
  - *Cross Site Scripting (content sniffing)*
  - *X-Frame-Option Header Not Set*
  - *Possible Username or Password Disclosure*

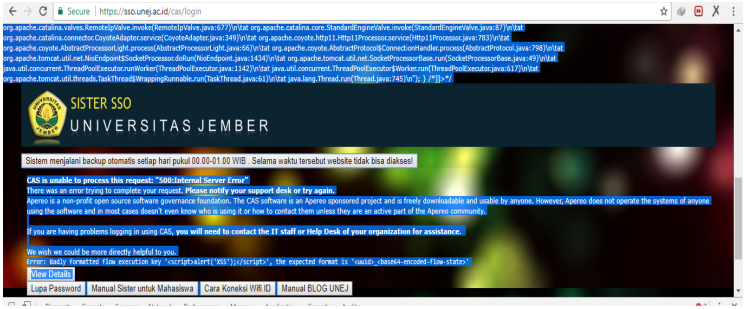
    - *Incomplete or No Cache-Control and Pragma HTTP Header Set*
- Sister.unej.ac.id
    - *Cross Site Scripting (verified)*
    - *Application Error Message*
    - *HTML Form without CSRF Protection*
    - *X-Frame-Option Header Not Set*
    - *Incomplete or No Cache-Control and Pragma HTTP Header Set*

6.4. Penetration Testing

Hasil *Penetration Testing* yang telah dilakukan dan dijelaskan pada bab V, didapat hasil yang beragam. Hasil dari celah yang telah diuji dijabarkan pada sub bab berikut ini.

6.4.1. "Application Error Message"

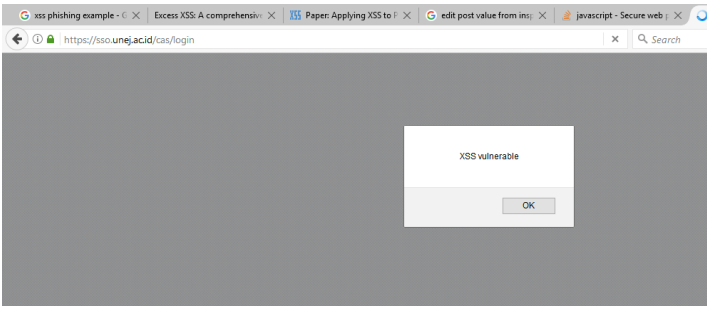
Pada celah ini terdapat *error message* yang muncul ketika menginputkan pada parameter tertentu yang terdapat pada halaman login. Penguji mengubah input dari parameter dengan bantuan menggunakan fitur *Inspect Element* pada *browser*. *Error Message* muncul namun tidak terdapat informasi sensitif yang muncul.



Gambar 6.1. Error Message pada sso.unej.ac.id

6.4.2. "Cross Site Scripting (content sniffing)"

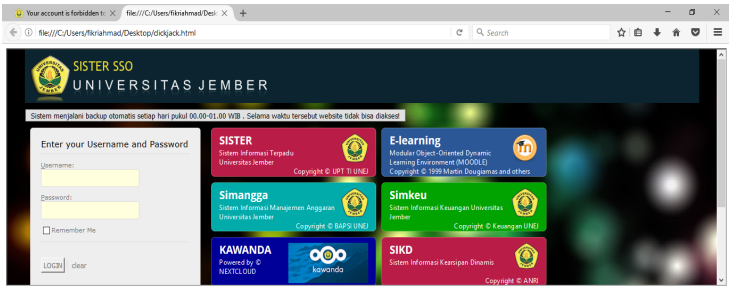
Pada celah XSS yang ditemukan pada sso.unej.ac.id berada pada halaman login. Yaitu pada attribute "_eventId". Ketika input diubah ke dalam bentuk script XSS maka muncul popup window hasil dari script. Celah ini juga rentan terhadap XSS phising. Karena adanya XSS ini, seorang hacker dapat mengakses halaman sukses login walaupun tidak benar-benar masuk ke dalam sso. Hal ini dapat digunakan untuk tools social engineering dimana hacker membuat web phising untuk menyimpan username dan password namun tetap mengarahkan korban ke halaman sukses login. Sehingga korban tidak menyadari bahwa hak aksesnya telah dicuri. Celah ini dapat terjadi juga diakibatkan tidak adanya XSRF protection pada sso.unej.ac.id sehingga POST yang masuk dari web phising diterima dan diproses.



Gambar 6.2. pengujian xss pada sso.unej.ac.id

6.4.3. "X-Frame-Option Header Not Set"

Pengujian pada celah ini dilakukan dengan cara membuat script sederhana dan membuat iframe yang bersumber pada sso.unej.ac.id dan Iframe berhasil muncul. Celah ini cukup berbahaya karena dapat digunakan sebagai tools untuk *social engineering*.



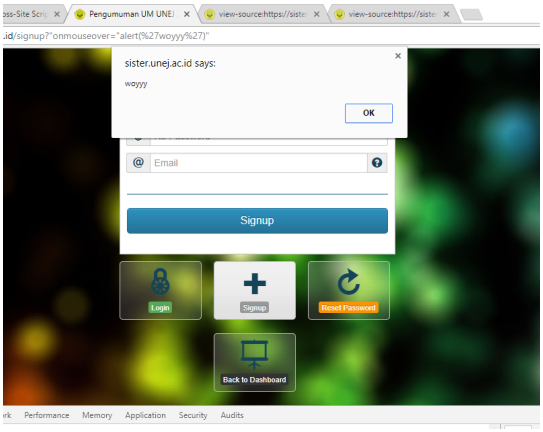
Gambar 6.3. Clickjacking pada sso.unej.ac.id

6.4.4. “Possible Username or Password Disclosure”

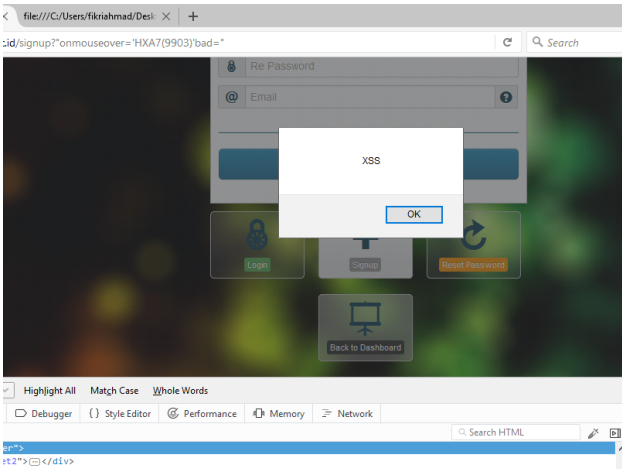
Pengujian pada celah ini dilakukan dengan cara mengakses file yang terindikasi menampil konten sensitif. Ternyata konten tersebut bukan password melainkan bagian dari script pada file css.

6.4.5. “Cross Site Scripting (verified)”

Pada celah XSS yang ditemukan pada sister.unej.ac.id berada pada halaman recovery dan halaman sign up. Kerentanan XSS ditemukan pada attribute “onmouseover”. Pada halaman recovery, muncul popup window alert ketika mouse diarahkan ke tombol “back to dashboard”. Pada halaman signup ketika dimasukkan script yang sama, maka akan muncul pop window ketika mouse diarahkan ke tombol “back to dashboard”



Gambar 6.4. XSS pada halaman recovery



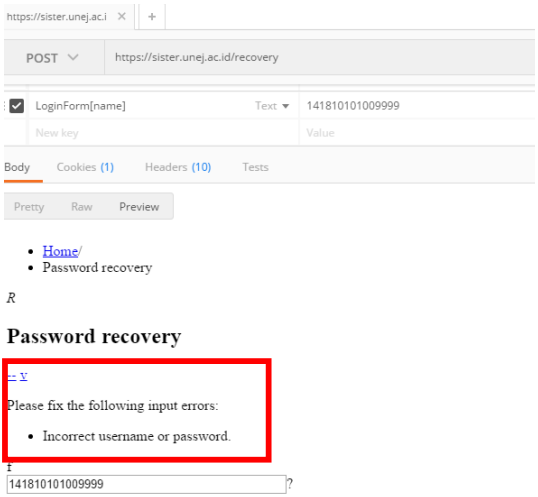
Gambar 6.5. XSS pada halaman signup

6.4.6. "Application Error Message"

Pada celah ini dilakukan pengujian dengan bantuan fitur Inspect Element pada browser pada sister.unej.ac.id halaman recovery dan signup. Penguji menginputkan random script pada parameter yang diduga pemicu error message. Maka error message pun muncul.

6.4.7. "HTML Form without CSRF Protection"

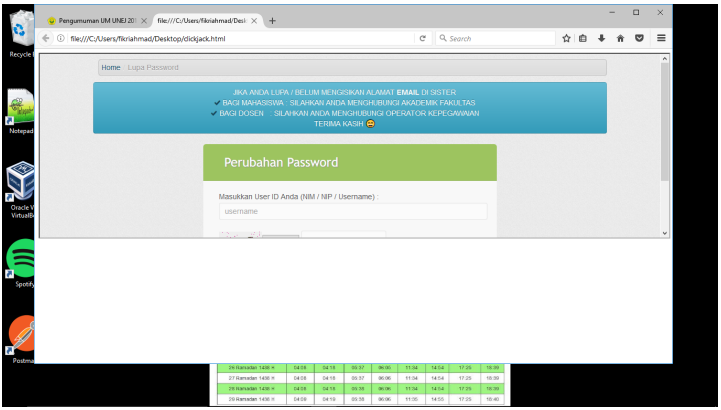
Pada pengujian celah ini dilakukan dengan bantuan aplikasi postman. Aplikasi postman mengirimkan sebuah request pada halaman yang terindikasi memiliki celah CSRF yaitu halaman recovery dan signup. Hasilnya request diterima dan diproses. Namun ternyata halaman yang terindikasi rentan CSRF, tidak digunakan lagi oleh sister.



Gambar 6.6. CSRF pada halaman recovery

6.4.8. "X-Frame-Option Header Not Set"

Pada celah ini penguji membuat file html sederhana yang berisi iframe dengan source sister.unej.ac.id/lupapassword. ketika file dijalankan muncul halaman tersebut. Hal ini cukup berbahaya karena dapat digunakan untuk clickjacking dan tool untuk social engineering.



Gambar 6.7. clickjacking pada sister.unej.ac.id

6.4.9. "Incomplete or No Cache-Control and Pragma HTTP Header Set"

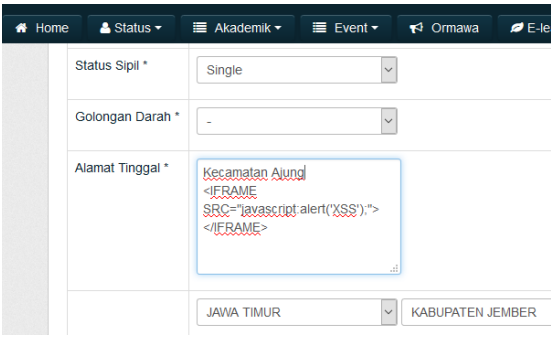
Pada celah ini dilakukan pengujian dengan melihat page source dari halaman yang diduga tidak terdapat *cache-control*. Tidak adanya cache-control memang mempercepat loading dari browser ketika mengakses website, namun ditakutkan file tersebut mengandung informasi sensitif. Ketika diteliti ternyata file tersebut merupakan file css dan tidak mengandung informasi sensitif.

6.5. Eksploitasi Celah

Dari tahap eksploitasi celah, penguji mendapatkan hak akses dari salah satu mahasiswa Universitas Jember. Ketika diakses, tidak banyak yang dapat dilakukan penguji karena pada dasarnya, informasi yang muncul bersifat permanen dan tidak dapat diubah. Terdapat form biodata pada Sister dan ketika

diujikan ternyata form rentan terhadap XSS dimana saat diuji dapat memunculkan window alert. Selain itu ditemukan celah lain yang terdapat pada sister yaitu *Clickjacking* pada halaman kuliah/dashboard. Namun hal ini tidak dapat digunakan karena untuk mengakses halaman tersebut perlu adanya login pada sso.unej.ac.id.

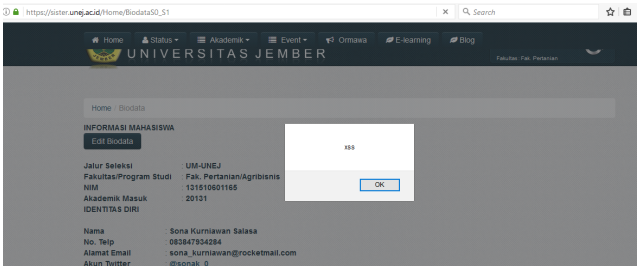
Gambar 6.8. web phising untuk mendapatkan akses



Gambar 6.9. pengujian pada form biodata

```
<td width='8'>:
</td>
<td><b></script><script>alert('xss')</script><script></b>
</td>
```

Gambar 6.10. pengujian pada form biodata



Gambar 6.11. Hasil Pengujian XSS

6.6. Analisis Hasil Pengujian

Pada tahap ini, penguji akan melakukan analisis hasil pengujian yang telah dilakukan pada tahapan - tahapan sebelumnya. Penguji akan membuat hasil pengujian terhadap celah serta

membuat rekomendasi perbaikan terhadap sistem dari celah yang ditemukan. Ringkasan tahap pengujian dijelaskan pada table 6.12 dan hasil pengujian dijelaskan pada table 6.13 dan table 6.14.

Table 6.12. Ringkasan Pengujian sso.unej.ac.id

No	Celah Keamanan	Dampak	Hasil pengujian
1	Cross Site Scripting (Content Sniffing)	Dapat merubah tampilan web, menyisipkan link ke site lain.	Parameter yang diduga rentan XSS diinputkan dengan bantuan Inspect Element. Hasil dari XSS muncul error message.
2	Application Error Message	Dapat memunculkan informasi sensitif. Namun setelah diuji, error message tidak menimbulkan informasi sensitif.	Tidak ditemukannya informasi sensitif pada *error message* yang muncul.
3	X-Frame-Option Header Not Set	Web dapat disematkan kedalam iframe dan dapat digunakan untuk social engineering	Pengujian dilakukan dan website sso.unej.ac.id muncul di dalam iframe
4	Incomplete or No Cache-Control and	Dapat mengandung informasi/konten sensitif.	File yang tidak terdapat cache-control merupakan file css yang

No	Celah Keamanan	Dampak	Hasil pengujian
	Pragma HTTP Header Set		tidak mengandung konten sensitif.
5	Possible Username or Password Disclosure	Dapat mengandung informasi/konten sensitif.	Informasi yang diduga merupakan password ternyata merupakan bagian dari script css.

Table 6.13. Ringkasan Pengujian sister.unej.ac.id

No	Celah Keamanan	Dampak	Hasil pengujian
1	Application Error Message	Dapat memunculkan informasi sensitif. Namun setelah diuji, error message tidak menimbulkan informasi sensitif.	Tidak ditemukannya informasi sensitif pada *error message* yang muncul. *Error message* pun tidak muncul
2	Cross Site Scripting (Verified)	Dapat merubah tampilan web, menyisipkan link ke site lain.	parameter yang diduga rentan XSS yaitu “onmouseover” pada halaman recovery dan signup, terbukti rentan terhadap XSS.

No	Celah Keamanan	Dampak	Hasil pengujian
3	HTML Form without CSRF Protection	Web dapat menerima unauthorized request dari luar web	Pengujian denga postman membuktikan post diproses oleh server. Walaupun halaman yang rentan CSRF sudah tidak digunakan.
4	X-Frame-Option Header Not Set	Web dapat disematkan kedalam iframe dan dapat digunakan untuk social engineering	Pengujian dilakukan dan website sso.unej.ac.id muncul di dalam iframe
3	Incomplete or No Cache-Control and Pragma HTTP Header Set	Dapat mengandung informasi/konten sensitif.	File yang tidak terdapat cache-control merupakan file css yang tidak mengandung konten sensitif.
4	Email Address Found	Mengandung email yang dapat disalahgunakan	Email yang ditemukan acunetix merupakan email yang terdapat pada file javascript dimana email tersebut merupakan email creator dari javascript tersebut

Table 6.14. Ringkasan tahap pengujian

No	Tahapan	Status	Deskripsi
1	Pengintaian Sistem	Dilaksanakan	Pengintaian dilakukan dengan bantuan Zenmap
2	Pencarian Celah	Dilaksanakan	Vulnerability Scanning dilakukan dengan 5 tools yaitu Acunetix, ZAP, W3af, Burp Suite, dan Nessus
3	Analisis dan Perencanaan Pengujian	Dilaksanakan	Menentukan celah yang akan diuji pada tahapan *penetration testing*
4	Penetration Testing	Dilaksanakan	Penetration Testing dilakukan secara manual terhadap celah yang telah ditentukan pengujiannya.
5	Eksploitasi Celah	Dilaksanakan	Eksploitasi celah yang dapat dilakukan sebatas dari privilege mahasiswa seperti

			melakukan perubahan informasi biodata. Pada biodata tidak dapat disematkan script karena terdapat sudah terdapat filter.
6	Analisis Hasil Pengujian	Dilaksanakan	Analisis dilakukan dari dampak serta hasil penetration testing pada celah. Serta perumusan rekomendasi perbaikan celah.
7	Clean Up Sistem	Dilaksanakan	Permbersihan dilakukan pada form biodata yang awalnya informasi diubah untuk keperluan pengujian.

6.7. Rekomendasi Perbaikan Celah

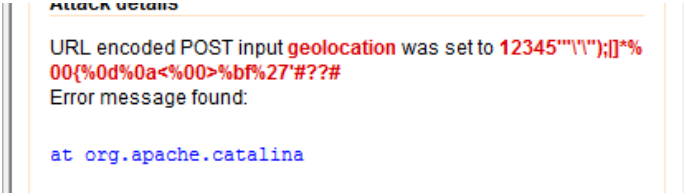
Rekomendasi perbaikan akan dibagi menjadi 2 bagian berdasarkan pada dimana celah website yang telah diuji sebelumnya.

6.7.1. Sso.unej.ac.id

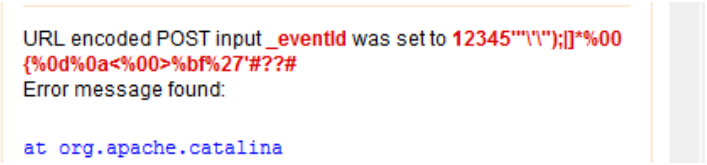
Berikut penguji rumuskan rekomendasi perbaikan terhadap website sso.unej.ac.id berdasarkan celah yang telah ditemukan pada tahap Pencarian Celah. Celah yang dijelaskan berikut telah

diurutkan dengan format dari ranking vulnerability tinggi ke rendah

- Application Error Message
  Untuk celah keamanan ini, terjadi ketika kita mengubah *variable post input* dengan berbagai macam karakter. Dimana *error message* muncul karena web tidak dapat memproses input yang dimasukkan. Rekomendasi yang berikan adalah untuk melakukan *filter input* karakter atau membatasi jumlah input hingga hanya beberapa karakter. Selain itu UPT TI Universitas Jember juga dapat membuat *script* dimana ketika *error page* diakses maka otomatis akan me-*redirect* ke *page* lain.



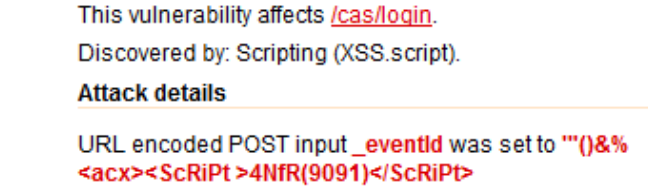
Gambar 6.12. penyebab error message



Gambar 6.13. penyebab error message

- Cross Site Scripting (content sniffing)

Sama halnya dengan error message, celah ini muncul ketika ketika mengubah post input dari “eventId”. Cross site scripting dapat dihalang dengan cara melakukan filter metacharacter pada input form. Langkah paling mudah yang dapat dilakukan adalah menggunakan fitur **htmlspecialchar()** pada php. Sehingga ketika menginputkan karakter non alphabet, karakter tersebut dapat di parse dan tidak dibaca oleh server sebagai javascript.



Gambar 6.14. penyebab XSS (content sniffing)

- X-Frame-Option Header Not Set
  Untuk celah keamanan ini, dapat diperbaiki dengan melakukan set pada X-frame-Option Header. Dari hasil *port scanning*, ditemukan bahwa Sister Universitas Jember menggunakan server apache dan nginx maka perlu dilakukan hal berikut.
  Apache
  untuk melakukan set X-frame-Option pada apache, inputkan dua *script* dibawah ini pada site configuration:

```
1 | Header always append X-Frame-Options SAMEORIGIN
```

Gambar 6.15. script X-frame-options

```
1 | Header set X-Frame-Options DENY
```

Gambar 6.16. script X-frame-options

Nginx

Untuk melalukan set X-Frame-Options header maka, tambahkan script pada gambar 15 di http, server, atau site configuration.

```
1 | add_header X-Frame-Options SAMEORIGIN;
```

Gambar 6.17. script X-frame-options

- Incomplete or No Cache-Control and Pragma HTTP Header Set
  Pada celah ini, ditemukan bahwa yang tidak memilik *cache-control* adalah file css. Ini mungkin sengaja dilakukan agar mempercepat *loading* website ketika diakses. Namun jika tidak, disarankan untuk menambahkan *code* untuk melakukan set cache control dan Pragma HTTP header pada file htaccess.

```
<IfModule mod_headers.c>
    Header set Cache-Control "no-cache, no-store, must-revalidate"
    Header set Pragma "no-cache"
    Header set Expires 0
</IfModule>
```

Gambar 6.18. script cache-control dan pragma header

- Web Browser XSS Protection Not Enabled
  Celah ini ditemukan, karena tidak terdapat XSS protection pada website, disarankan untuk mengaktifkan pengaman ini dengan cara menambahkan code pada file htacess seperti pada gambar 6.10.

```
X-XSS-Protection: 1, mode=block
```

Gambar 6.19. Script XSS protection

- X-Content-Type-Options Header Missing
  Pada celah keamanan ini, disarankan untuk menambahkan code pada file konfigurasi htaccess yang digunakan Sister Universitas Jember seperti yang ada pada gambar 18.

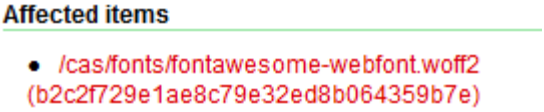
```
<IfModule mod_header.c>
Header set X-Content-Type-Options nosniff
</IfModule>
```

Gambar 6.20. Script X-Content-Type-Options

- Possible Username or Password disclosure

Celah ini, merupakan salah satu celah *false positive* yang ditemukan oleh acunetix. Celah ini bersifat *informational* sehingga celah ini tidak membahayakan dan tidak perlu adanya perbaikan lebih lanjut.

- Broken Links
  Celah ini mengindikasikan adanya file yang tidak dapat diakses. Celah ini bersifat Informational sehingga tidak terlalu membahayakan. Saran perbaikan yang penulis berikan adalah menghapus link/file tersebut sehingga tidak dapat diakses ataupun membuat file tersebut dapat diakses user bila diperlukan.



Gambar 6.21. celah broken links

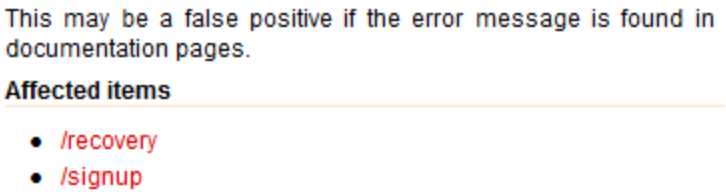
6.7.2. Sister.unej.ac.id

Berikut penguji rumuskan rekomendasi perbaikan terhadap website sister.unej.ac.id berdasarkan celah yang telah ditemukan pada tahap Pencarian Celah. Celah yang dijelaskan berikut telah diurutkan dengan format dari ranking vulnerability tinggi ke rendah.

- Cross Site Scripting(verified)
  Cross site scripting dapat dihalang dengan cara melakukan filter metacharacter pada input form. Langkah paling mudah yang dapat dilakukan adalah

menggunakan fitur **htmlspecialchars()** pada php. Sehingga ketika menginputkan karakter *non-alphabet*, karakter tersebut dapat di parse dan tidak dibaca oleh server sebagai javascript.

- Application Error Message
- Untuk celah keamanan ini, terjadi ketika kita mengubah *variable post input* dengan berbagai macam karakter. Dimana *error message* muncul karena web tidak dapat memproses input yang dimasukkan. Rekomendasi yang berikan adalah untuk melakukan *filter input* karakter atau membatasi jumlah input hingga hanya beberapa karakter. Selain itu UPT TI Universitas Jember juga dapat membuat *script* dimana ketika *error page* diakses maka otomatis akan me-*redirect* ke *page* lain.

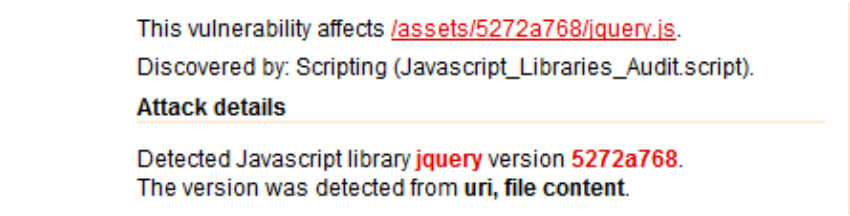


Gambar 6.22. celah ditemukan error messages

- HTML Form without CSRF Protection
  Untuk celah keaman ini, penulis menyarankan untuk membuat token pada setiap request dan menghubungkannya dengan user's session. Dengan adanya token web dapat memastikan permintaan

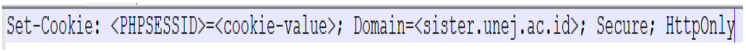
tersebut berasal dari user. Penulis juga menyarankan untuk penggunaan *captcha* pada form login.

- Vulnerable Javascript Library
  Celah ini mengindikasikan bahwa website Sister Universitas Jember menggunakan javascript yang sudah *out-of-dated*. Saran dari penulis untuk memperbaiki celah ini adalah mengganti / melakukan update terhadap javascript yang telah digunakan tersebut.



Gambar 6.23. file javascript yang vulnerable

- X-Frame-Option Header Missing
  Untuk celah ini, penulis menyarankan melakukan hal yang sama yang telah dijelaskan pada celah sso.unej.ac.id
- Cookie Without Httponly Flag Set
  Pada celah ini, penulis menyarankan untuk melakukan set terhadap cookie agar hanya bisa diakses oleh selain website sister. Untuk melakukan set httponly maka perlu adanya script tambahan yang dapat ditambahkan pada file htaccess ataupun httpd.conf seperti pada gambar 7.



Gambar 6.24. script set httponly pada cookie.

- Cookie Without Secure Flag
  Pada celah ini, penulis menyarankan hal yang sama seperti pada celah sebelumnya. Dimana perlu adanya script tambahan.
- Incomplete or No Cache-Control and Pragma HTTP Header Set
  Untuk celah ini, penulis menyarankan melakukan hal yang sama yang telah dijelaskan pada celah sso.unej.ac.id
- Web Browser XSS Protection Not Enabled
  Untuk celah ini, penulis menyarankan melakukan hal yang sama yang telah dijelaskan pada celah sso.unej.ac.id.
- X-Content-Type-Options Header Missing
  Untuk celah ini, penulis menyarankan melakukan hal yang sama yang telah dijelaskan pada celah sso.unej.ac.id
- Password Type Input with auto-completed enabled
  Pada celah keamanan ini, penulis menyarankan untuk melakukan *set autocomplete off* pada form. Pada tahap percobaan muncul pop up window yang mengijinkan untuk menyimpan *username* dan *password*. Hal ini berbahaya jika terdapat user yang menggunakan komputer bersama seperti di Lab ataupun warnet.
- Email Found

Pada celah ini bersifat informational dimana dikategorikan celah yang tidak berbahaya terhadap web. Setelah penulis uji ternyata email yang ditemukan merupakan creator dari file css yang digunakan Sister Universitas Jember.

6.7.3. Eksploitasi Celah

Pada saat eksploitasi celah, ditemukan kerentanan antara lain Clickjacking dan XSS. Untuk Clickjacking tidak berbahaya karena ketika menyematkan link sister pada iframe, link tersebut akan redirect ke halaman login sso. Untuk Celah XSS, perlu adanya filter meta character. Sama seperti rekomendasi sebelumnya, penguji menyarankan untuk menggunakan fitur **htmlspecialchar()** pada semua form yang dapat menyimpan sebuah input dari user.

6.8. Clean Up Sistem

Pada tahap Clean Up sistem (pembersihan) penguji merubah kembali semua informasi yang sebelumnya diubah pada saat ekploitasi celah.

(Halaman ini sengaja dikosongkan)

BAB VII
KESIMPULAN DAN SARAN

Pada bab ini dijelaskan kesimpulan dan saran yang dapat diambil dari pengujian – pengujian yang telah dilakukan. Kesimpulan dan saran yang dirumuskan nantinya dapat diimplementasikan oleh pihak Universitas Jember untuk memperbaiki Sister Universitas Jember.

7.1. Kesimpulan

Pada bagian ini akan dijabarkan mengenai kesimpulan – kesimpulan yang penguji dapat dari melaksanakan pengujian serta menjawab rumusan masalah yang telah dibuat sebelumnya. Kesimpulan yang didapat adalah sebagai berikut.

1. Pada Sister Universitas Jember telah ditemukan beberapa celah yang telah dipaparkan pada Bab VI namun tidak dapat dieksplotasi lebih lanjut.
2. Terdapat beberapa dampak dari celah yang telah ditemukan dan telah dipaparkan pada Bab VI subbab Analisis hasil pengujian dimana pada subbab tersebut dijelaskan dampak yang diperkirakan dan hasil pengujian terhadap dampak yang ada.
3. Solusi terhadap semua celah yang ditemukan pada pengujian dirumuskan pada bab VI pada subbab Analisis Hasil Pengujian, dimana dipaparkan rekomendasi perbaikan yang perlu dilakukan terhadap sistem informasi terpadu Universitas Jember.

7.2. Saran

Penulis akan merumuskan beberapa saran yang mengacu pada penelitian yang telah dilaksanakan. Saran yang penulis berikan dibagi menjadi dua, yaitu untuk pihak Universitas Jember terkait dengan hasil dari pengujian, dan untuk pihak yang akan melakukan penelitian terkait ataupun sesuai dengan ranah penelitian.

Saran yang diberikan terhadap pihak Universitas Jember adalah sebagai berikut:

1. Penulis menyarankan Universitas Jember untuk hasil rekomendasi yang telah disusun, diimplementasikan. Hal ini bertujuan untuk mencegah celah yang ada agar tidak dieksploitasi pihak lain serta meningkatkan kualitas keamanan dari Sister Universitas Jember.
2. Penulis menyarankan Univeristas Jember agar rekomendasi perbaikan diimplementasikan dengan menyesuaikan keadaan sistem yang sesungguhnya. Hal ini dikarenakan dalam rekomendasi yang disusun, penulis membuat berdasarkan celah yang ada, bukan berdasarkan keadaan sistem sesungguhnya.
3. Penulis menyarankan UPT TI Universitas Jember agar sering memperbaharui keamanan website dengan sering melakukan uji celah keamanan setiap kali terdapat pembaharuan fitur maupun tampilan.

Saran yang penulis berikan untuk penelitian selanjutnya adalah sebagai berikut:

1. Pengujian yang dilakukan penulis hanya sebatas pembuatan dokumen hasil pengujian evaluasi keamanan dan rekomendasi perbaikan. Hasil rekomendasi perbaikan yang penulis sampaikan tidak ditindaklanjuti atau dipantau lebih lanjut oleh penulis karena tidak diberikannya hak akses terhadap source code dari sistem tersebut. Ada baiknya peneliti berikut nya agar dapat memiliki hak akses terhadap sistem yang diuji sehingga rekomendasi yang diberikan terhadap sistem menjadi lebih detail dan akurat.
2. Pada proses pelaksanaan ujian perlu adanya perjanjian yang perlu dipahami bersama antara penguji dengan pihak objek pengujian terkait agar tidak adanya kesalahpahaman antara kedua belah pihak. Penguji harus memahami batasan batasan yang diberikan oleh pihak terkait sehingga dalam pengujian tidak mengganggu proses berlangsungnya website.
3. Pada pelaksanaan pengujian, jika terdapat celah yang tidak terdeteksi oleh *tools* aplikasi yang digunakan, disarankan untuk tetap diuji dan dicantumkan pada laporan tugas akhir.

(Halaman ini sengaja dikosongkan)

DAFTAR PUSTAKA

[1] S. Aswati, N. Mulyani, Y. Siagian dan A. Z. Syah, "Peranan Sistem Informasi dalam Perguruan TInggi," *Jurnal Teknologi dan Sistem Informasi,* vol. 1, pp. 79-86, 2015.

[2] Symantec, "Symantec Internet Security Threat Report," 2015. [Online]. Available: https://www4.symantec.com/mktginfo/whitepaper/ISTR/21347932_GA-internet-security-threat-report-volume-20-2015-social_v2.pdf.

[3] J. N. Goel dan B. Mehtre, "Vulnerability Assessment & Penetration Testing as a Cyber Defence Technology," *Procedia Computer Science 57,* pp. 710-715, 2015.

[4] Engrebeston, P. (2011). *The Basics of Hacking and Penetration Testing.* Waltham, Massachusetts: Elsevier Inc

[5] EC-Council, Penetration Testing Procdures & Methodologies, New York: Cengage Learning, 2011

[6] R. Vibhandik, dan A. K. Bose. "Vulnerability assessment of web applications - a testing approach." *2015 Forth International Conference on e-Technologies and Networks for Development (ICeND)*

[7] E. Karim. "Behavior Analysis of Malware in Institut Teknologi Sepuluh Nopember Surabaya, Indonesia", 2015

[8] A. Rahadiyan Danar dan S. Apol Pribadi, "Evaluasi Risiko Celah Keamanan Menggunakan Metodologi Open Web Application Security Project (OWASP) pada Aplikasi Web Sistem Informasi Mahasiswa (Studi Kasus: Perguruan Tinggi XYZ)", 2016

[9] S. Andrianto dan S. Apol Pribadi, "Pengujian dan Evaluasi Celah Keamanan Sistem Informasi Kepegawaian Peguruan Tinggi XYZ Menggunakan Kerangka Kerja VAPT", 2016

(Halaman ini sengaja dikosongkan)

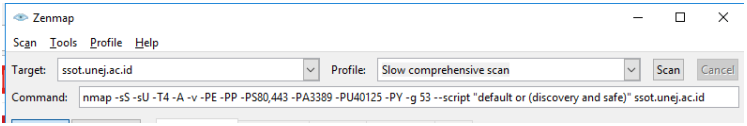
BIODATA PENULIS

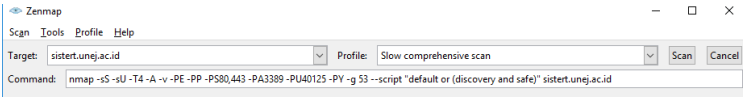
Penulis, Ahmad Fikri Zulfi, lahir di Jember, 17 April 1995, merupakan anak ketiga dan terakhir. Penulis telah menempuh pendidikan formal di SD Al-Furqan Jember, Jawa Timur, SMPN 1 Jember, Jawa Timur, SMAN 1 Jember, Jawa Timur. Pada tahun 2013 penulis diterima pada Jurusan Sistem Informasi FTIf – Institut Teknologi Sepuluh Nopember (ITS) Surabaya. Penulis berkesempatan mengikuti beberapa kegiatan kemahasiswaan seperti menjadi Staff Biro Komunikasi pada periode 2014/2015, menjadi kepala divisi internal Dalam Negeri pada perode 2015/2016, menjadi ketua komisi pemilihan ketua HIMASA 2016. Pada tahun 2016, penulis mendapatkan kesempatan untuk magang di PT. Telekomunikasi Selular (Telkomsel) Regional Sumatra Bagian Tengah di Batam selama 2 bulan.

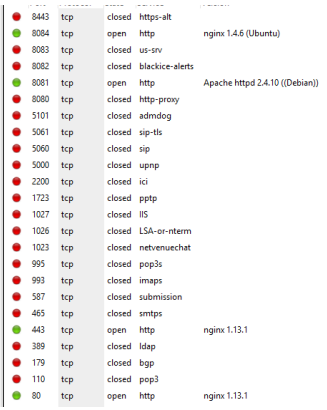
Penulis meng ambil bidang minat Infrastukru dan Keamanan Teknologi Informasi (IKTI) di Jurusan Sistem Informasi ITS. Untuk keperluan penelitian, penulis dapat dihubungi melalui email ahmadfikrizulfi@gmail.com.

LAMPIRAN A

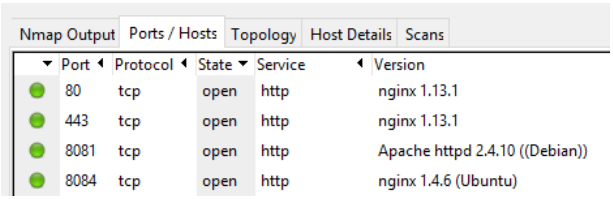
Pada lampiran A berisi tentang dokumentasi dari pengujian yang dilakukan penulis. Dokumentasi meliputi kegiatan dari pengintaian sistem hingga analisis hasil pengujian.





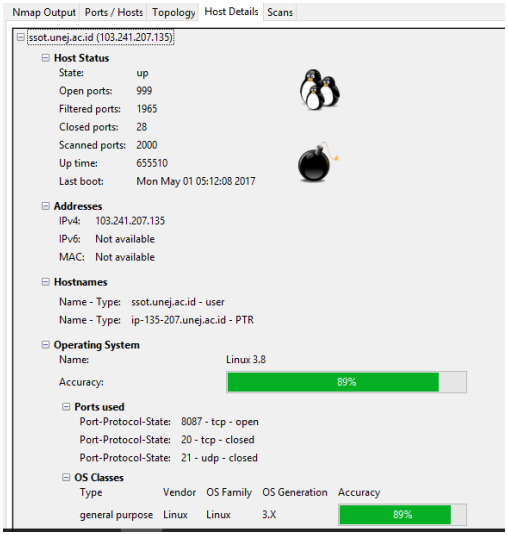


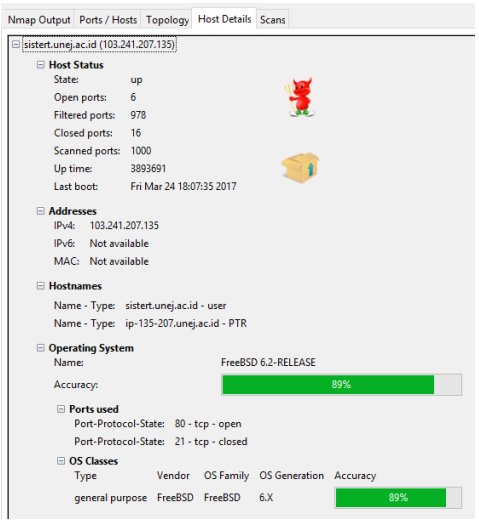
8443	tcp	closed	https-alt	
8084	tcp	open	http	nginx 1.4.6 (Ubuntu)
8083	tcp	closed	us-srv	
8082	tcp	closed	blackice-alerts	
8081	tcp	open	http	Apache httpd 2.4.10 ((Debian))
8080	tcp	closed	http-proxy	
5101	tcp	closed	admdog	
5061	tcp	closed	sip-tls	
5060	tcp	closed	sip	
5000	tcp	closed	upnp	
2200	tcp	closed	ici	
1723	tcp	closed	pptp	
1027	tcp	closed	IIS	
1026	tcp	closed	LSA-or-nterm	
1023	tcp	closed	netvenuechat	
995	tcp	closed	pop3s	
993	tcp	closed	imaps	
587	tcp	closed	submission	
465	tcp	closed	smtps	
443	tcp	open	http	nginx 1.13.1
389	tcp	closed	ldap	
179	tcp	closed	bgp	
110	tcp	closed	pop3	
80	tcp	open	http	nginx 1.13.1

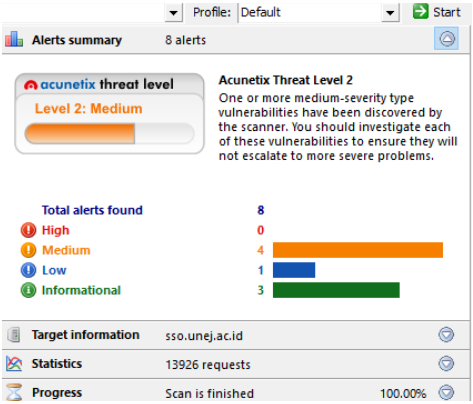


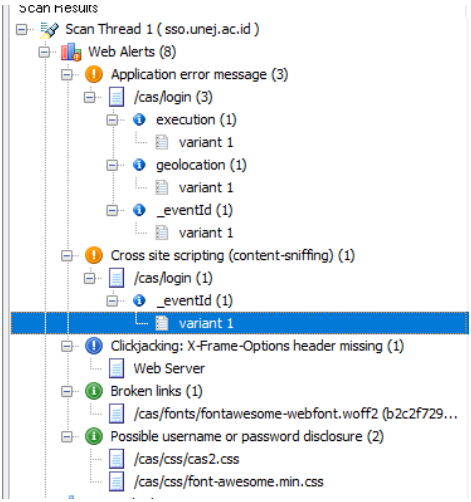
Nmap Output | Ports / Hosts | Topology | Host Details | Scans

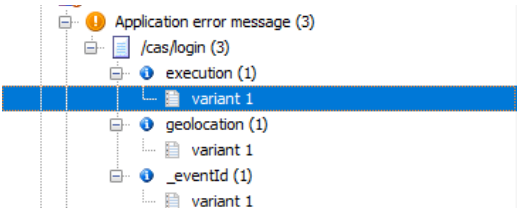
Port	Protocol	State	Service	Version
80	tcp	open	http	nginx 1.13.1
443	tcp	open	http	nginx 1.13.1
8081	tcp	open	http	Apache httpd 2.4.10 ((Debian))
8084	tcp	open	http	nginx 1.4.6 (Ubuntu)


Nmap Output
Ports / Hosts
Topology
Host Details
Scans
ssot.unej.ac.id (103.241.207.135)
Host Status
State: up
Open ports: 999
Filtered ports: 1965
Closed ports: 28
Scanned ports: 2000
Up time: 655510
Last boot: Mon May 01 05:12:08 2017
Addresses
IPv4: 103.241.207.135
IPv6: Not available
MAC: Not available
Hostnames
Name - Type: ssot.unej.ac.id - user
Name - Type: ip-135-207.unej.ac.id - PTR
Operating System
Name: Linux 3.8
Accuracy: 89%
Ports used
Port-Protocol-State: 8087 - tcp - open
Port-Protocol-State: 20 - tcp - closed
Port-Protocol-State: 21 - udp - closed
OS Classes
Type Vendor OS Family OS Generation Accuracy
general purpose Linux Linux 3.X 89%


Nmap Output
Ports / Hosts
Topology
Host Details
Scans
sistert.unej.ac.id (103.241.207.135)
Host Status
State: up
Open ports: 6
Filtered ports: 978
Closed ports: 16
Scanned ports: 1000
Up time: 3893691
Last boot: Fri Mar 24 18:07:35 2017
Addresses
IPv4: 103.241.207.135
IPv6: Not available
MAC: Not available
Hostnames
Name - Type: sistert.unej.ac.id - user
Name - Type: ip-135-207.unej.ac.id - PTR
Operating System
Name: FreeBSD 6.2-RELEASE
Accuracy: 89%
Ports used
Port-Protocol-State: 80 - tcp - open
Port-Protocol-State: 21 - tcp - closed
OS Classes
Type Vendor OS Family OS Generation Accuracy
general purpose FreeBSD FreeBSD 6.X 89%


Profile: Default
Start
Alerts summary
8 alerts
acunetix threat level
Level 2: Medium
Acunetix Threat Level 2
One or more medium-severity type vulnerabilities have been discovered by the scanner. You should investigate each of these vulnerabilities to ensure they will not escalate to more severe problems.
Total alerts found 8
High 0
Medium 4
Low 1
Informational 3
Target information sso.unej.ac.id
Statistics 13926 requests
Progress Scan is finished 100.00%


Scan Results
Scan Thread 1 (sso.unej.ac.id)
Web Alerts (8)
Application error message (3)
/cas/login (3)
execution (1)
variant 1
geolocation (1)
variant 1
_eventId (1)
variant 1
Cross site scripting (content-sniffing) (1)
/cas/login (1)
_eventId (1)
variant 1
Clickjacking: X-Frame-Options header missing (1)
Web Server
Broken links (1)
/cas/fonts/fontawesome-webfont.woff2 (b2c2f729...
Possible username or password disclosure (2)
/cas/css/cas2.css
/cas/css/font-awesome.min.css



Application error message

Severity MEDIUM

Vulnerability description

This page contains an error/warning message that may disclose sensitive information. The message can also contain the location of the file that produced the unhandled exception.

This may be a false positive if the error message is found in documentation pages.

This vulnerability affects /cas/login.

Discovered by: Scripting (Error_Message.script).

Attack details

URL encoded POST input **execution** was set to
Error message found:

```
at org.apache.catalina
```

Application error message

Severity MEDIUM

Vulnerability description

This page contains an error/warning message that may disclose sensitive information. The message can also contain the location of the file that produced the unhandled exception.

This may be a false positive if the error message is found in documentation pages.

This vulnerability affects /cas/login.

Discovered by: Scripting (Error_Message.script).

Attack details

URL encoded POST input **geolocation** was set to **12345'"\'\");[]*%00{%0d%0a<%00>%bf%27'#??#**
Error message found:

```
at org.apache.catalina
```

Application error message

Severity MEDIUM

Vulnerability description

This page contains an error/warning message that may disclose sensitive information. The message can also contain the location of the file that produced the unhandled exception.

This may be a false positive if the error message is found in documentation pages.

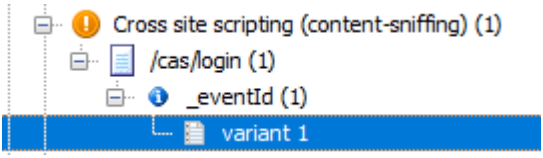
This vulnerability affects /cas/login.

Discovered by: Scripting (Error_Message.script).

Attack details

URL encoded POST input **_eventId** was set to **12345'"\'\");[]*%00{%0d%0a<%00>%bf%27'#??#**
Error message found:

```
at org.apache.catalina
```



Cross site scripting (content-sniffing)

Severity MEDIUM

Vulnerability description

This type of XSS can only be triggered on (and affects) content sniffing browsers.

This script is possibly vulnerable to Cross Site Scripting (XSS) attacks.

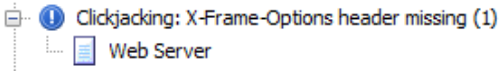
Cross site scripting (also referred to as XSS) is a vulnerability that allows an attacker to send malicious code (usually in the form of Javascript) to another user. Because a browser cannot know if the script should be trusted or not, it will execute the script in the user context allowing the attacker to access any cookies or session tokens retained by the browser.

This vulnerability affects /cas/login.

Discovered by: Scripting (XSS.script).

Attack details

URL encoded POST input **_eventId** was set to **'"()&%<acx><ScRiPt >4NfR(9091)</ScRiPt>**



Clickjacking: X-Frame-Options header mis Severity LOW

Vulnerability description

Clickjacking (User Interface redress attack, UI redress attack, UI redressing) is a malicious technique of tricking a Web user into clicking on something different from what the user perceives they are clicking on, thus potentially revealing confidential information or taking control of their computer while clicking on seemingly innocuous web pages.

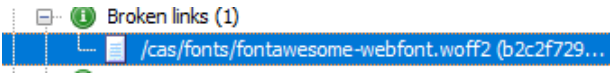
The server didn't return an **X-Frame-Options** header which means that this website could be at risk of a clickjacking attack. The X-Frame-Options HTTP response header can be used to indicate whether or not a browser should be allowed to render a page inside a frame or iframe. Sites can use this to avoid clickjacking attacks, by ensuring that their content is not embedded into other sites.

This vulnerability affects Web Server.

Discovered by: Scripting (Clickjacking_X_Frame_Options.script).

Attack details

No details are available.



Broken links Severity INFO

Vulnerability description

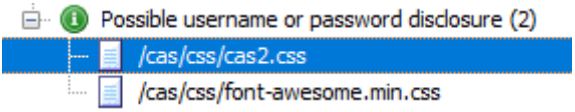
A broken link refers to any link that should take you to a document, image or webpage, that actually results in an error. This page was linked from the website but it is inaccessible.

This vulnerability affects /cas/fonts/fontawesome-webfont.woff2 (b2c2f729e1ae8c79e32ed8b064359b7e).

Discovered by: Crawler.

Attack details

For a complete list of URLs linking to this file, go to Site Structure > Locate and select the file (marked as "Not Found") > select Referrers Tab from the bottom of the Information pane.



Possible username or password disclosu Severity INFO

Vulnerability description

A username and/or password was found in this file. This information could be sensitive.

This alert may be a false positive, manual confirmation is required.

This vulnerability affects /cas/css/cas2.css.

Discovered by: Scripting (Text_Search_File.script).

Attack details

Pattern found:

```
pass:before
```

Possible username or password disclosu Severity INFO

Vulnerability description

A username and/or password was found in this file. This information could be sensitive.

This alert may be a false positive, manual confirmation is required.

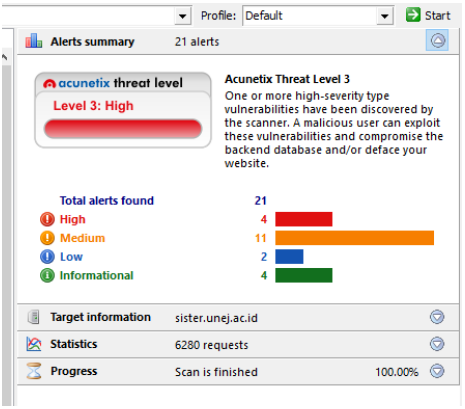
This vulnerability affects /cas/css/font-awesome.min.css.

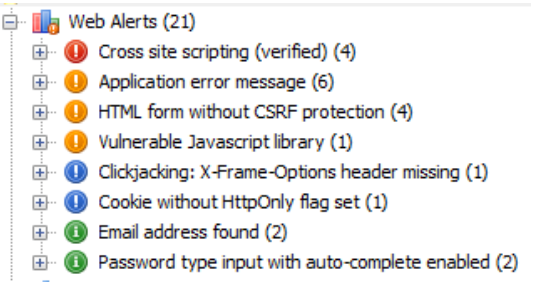
Discovered by: Scripting (Text_Search_File.script).

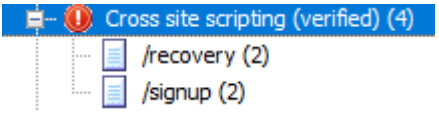
Attack details

Pattern found:

```
pass:before
```


Profile: Default
Start
Alerts summary
21 alerts
acunetix threat level
Level 3: High
Acunetix Threat Level 3
One or more high-severity type vulnerabilities have been discovered by the scanner. A malicious user can exploit these vulnerabilities and compromise the backend database and/or deface your website.
Total alerts found 21
High 4
Medium 11
Low 2
Informational 4
Target information sister.unej.ac.id
Statistics 6280 requests
Progress Scan is finished 100.00%


Web Alerts (21)
Cross site scripting (verified) (4)
Application error message (6)
HTML form without CSRF protection (4)
Vulnerable Javascript library (1)
Clickjacking: X-Frame-Options header missing (1)
Cookie without HttpOnly flag set (1)
Email address found (2)
Password type input with auto-complete enabled (2)


Cross site scripting (verified) (4)
/recovery (2)
/signup (2)

Cross site scripting (verified)

Severity HIGH

Vulnerability description

This script is possibly vulnerable to Cross Site Scripting (XSS) attacks.

Cross site scripting (also referred to as XSS) is a vulnerability that allows an attacker to send malicious code (usually in the form of Javascript) to another user. Because a browser cannot know if the script should be trusted or not, it will execute the script in the user context allowing the attacker to access any cookies or session tokens retained by the browser.

This vulnerability affects /recovery.

Discovered by: Scripting (XSS_in_URI_File.script).

Attack details

URI was set to **"onmouseover='kHlh(9657)'bad="**
The input is reflected inside a tag parameter between double quotes.

Cross site scripting (verified)

Severity HIGH

Vulnerability description

This script is possibly vulnerable to Cross Site Scripting (XSS) attacks.

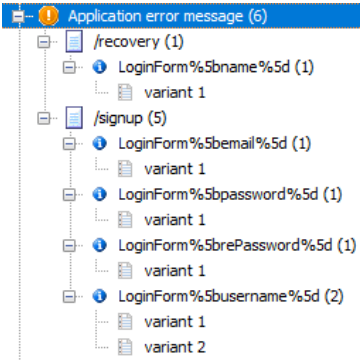
Cross site scripting (also referred to as XSS) is a vulnerability that allows an attacker to send malicious code (usually in the form of Javascript) to another user. Because a browser cannot know if the script should be trusted or not, it will execute the script in the user context allowing the attacker to access any cookies or session tokens retained by the browser.

This vulnerability affects /signup.

Discovered by: Scripting (XSS_in_URI_File.script).

Attack details

URI was set to **"onmouseover='HXA7(9903)'bad="**
The input is reflected inside a tag parameter between double quotes.



Application error message

Severity: MEDIUM

Vulnerability description

This page contains an error/warning message that may disclose sensitive information. The message can also contain the location of the file that produced the unhandled exception.

This may be a false positive if the error message is found in documentation pages.

This vulnerability affects /recovery.

Discovered by: Scripting (Error_Message.script).

Attack details

URL encoded POST input **LoginForm%5bname%5d** was set to **loesfnji**
Error message found:

```
Internal Server Error
```

Application error message

Severity: MEDIUM

Vulnerability description

This page contains an error/warning message that may disclose sensitive information. The message can also contain the location of the file that produced the unhandled exception.

This may be a false positive if the error message is found in documentation pages.

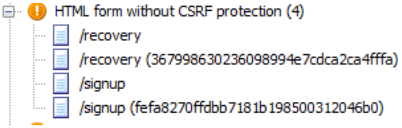
This vulnerability affects /signup.

Discovered by: Scripting (Error_Message.script).

Attack details

URL encoded POST input **LoginForm%5bemail%5d** was set to **sample%40email.tst**
Error message found:

```
Internal Server Error
```



HTML form without CSRF protection

Severity: MEDIUM

Vulnerability description

This alert may be a false positive, manual confirmation is required.

Cross-site request forgery, also known as a one-click attack or session riding and abbreviated as CSRF or XSRF, is a type of malicious exploit of a website whereby unauthorized commands are transmitted from a user that the website trusts.

Acunetix WVS found a HTML form with no apparent CSRF protection implemented. Consult details for more information about the affected HTML form.

This vulnerability affects /recovery.

Discovered by: Crawler.

Attack details

Form name: <empty>
Form action: https://sister.unej.ac.id/recovery
Form method: POST

Form inputs:

- LoginForm[name] [Text]
- yt0 [Submit]

HTML form without CSRF protection

Severity: MEDIUM

Vulnerability description

This alert may be a false positive, manual confirmation is required.

Cross-site request forgery, also known as a one-click attack or session riding and abbreviated as CSRF or XSRF, is a type of malicious exploit of a website whereby unauthorized commands are transmitted from a user that the website trusts.

Acunetix WVS found a HTML form with no apparent CSRF protection implemented. Consult details for more information about the affected HTML form.

This vulnerability affects /signup.

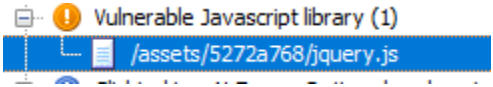
Discovered by: Crawler.

Attack details

Form name: <empty>
Form action: https://sister.unej.ac.id/signup
Form method: POST

Form inputs:

- LoginForm[username] [Text]
- LoginForm[password] [Password]
- LoginForm[rePassword] [Password]
- LoginForm[email] [Text]
- yt0 [Submit]



Vulnerable Javascript library

Severity: MEDIUM

Vulnerability description

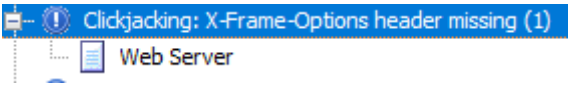
You are using a vulnerable Javascript library. One or more vulnerabilities were reported for this version of the Javascript library. Consult Attack details and Web References for more information about the affected library and the vulnerabilities that were reported.

This vulnerability affects /assets/5272a768/jquery.js.

Discovered by: Scripting (Javascript_Libraries_Audit.script).

Attack details

Detected Javascript library **jquery** version **5272a768**.
The version was detected from **uri, file content**.



Clickjacking: X-Frame-Options header mis

Severity: LOW

Vulnerability description

Clickjacking (User Interface redress attack, UI redress attack, UI redressing) is a malicious technique of tricking a Web user into clicking on something different from what the user perceives they are clicking on, thus potentially revealing confidential information or taking control of their computer while clicking on seemingly innocuous web pages.

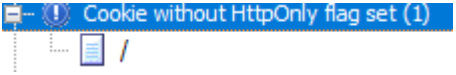
The server didn't return an **X-Frame-Options** header which means that this website could be at risk of a clickjacking attack. The X-Frame-Options HTTP response header can be used to indicate whether or not a browser should be allowed to render a page inside a frame or iframe. Sites can use this to avoid clickjacking attacks, by ensuring that their content is not embedded into other sites.

This vulnerability affects **Web Server**.

Discovered by: Scripting (Clickjacking_X_Frame_Options.script).

Attack details

No details are available.



Cookie without HttpOnly flag set

Severity: LOW

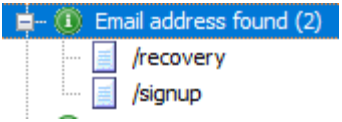
Vulnerability description

This cookie does not have the HTTPOnly flag set. When a cookie is set with the HTTPOnly flag, it instructs the browser that the cookie can only be accessed by the server and not by client-side scripts. This is an important security protection for session cookies.

Affected items

- /

The impact of this vulnerability



Email address found

Severity: INFO

Vulnerability description

One or more email addresses have been found on this page. The majority of spam comes from email addresses harvested off the internet. The spam-bots (also known as email harvesters and email extractors) are programs that scour the internet looking for email addresses on any website they come across. Spambot programs look for strings like myname@mydomain.com and then record any addresses found.

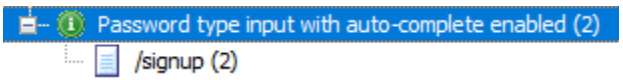
This vulnerability affects /recovery.

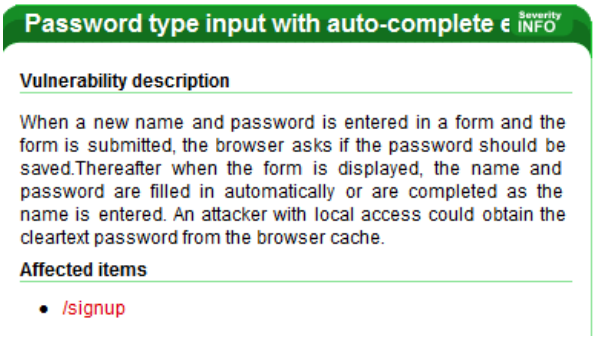
Discovered by: Scripting (Text_Search_File.script).

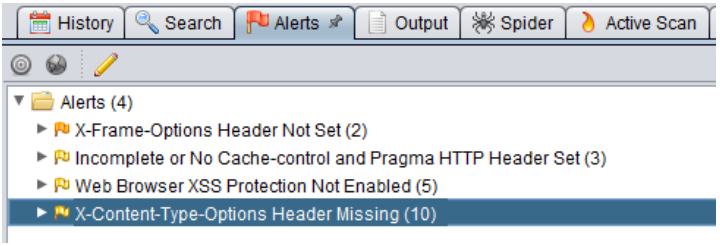
Attack details

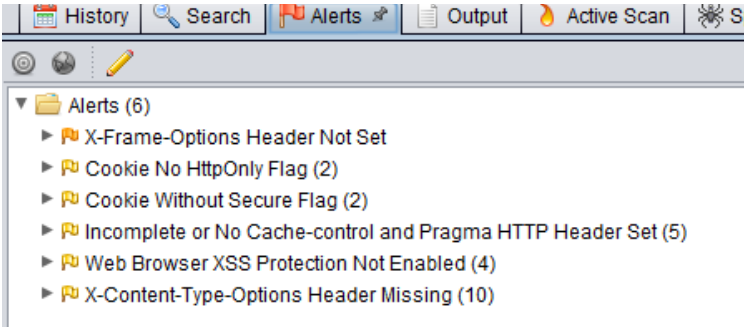
Pattern found:

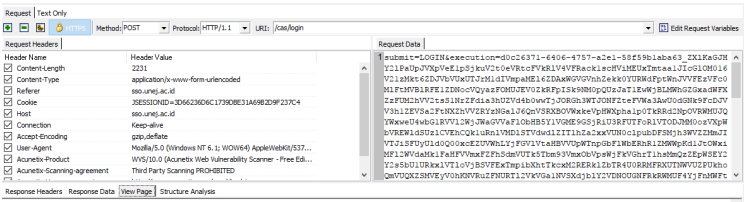
```
john.doe@mail.com
```

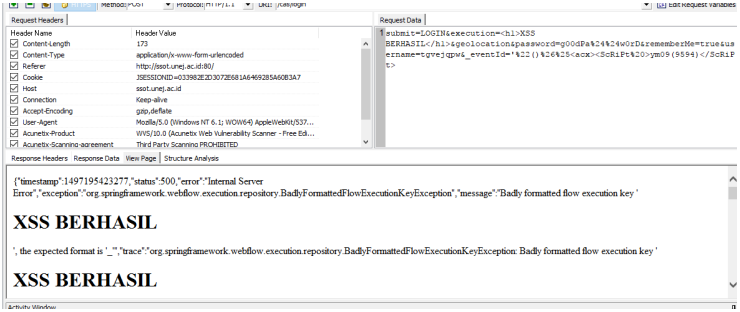


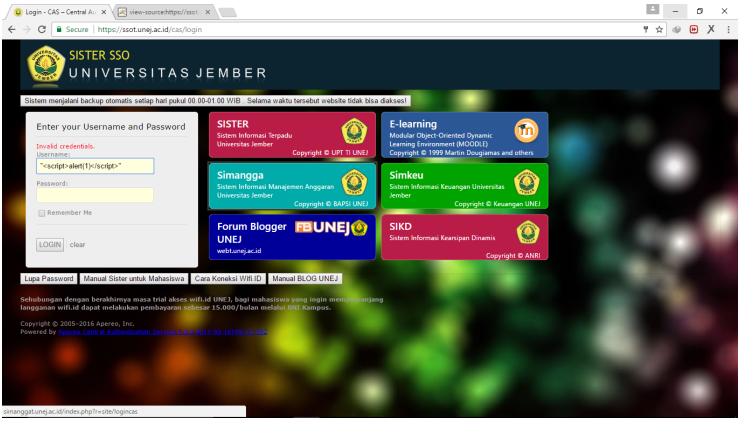

Password type input with auto-complete e
Severity
INFO
Vulnerability description
When a new name and password is entered in a form and the form is submitted, the browser asks if the password should be saved.Thereafter when the form is displayed, the name and password are filled in automatically or are completed as the name is entered. An attacker with local access could obtain the cleartext password from the browser cache.
Affected items
/signup

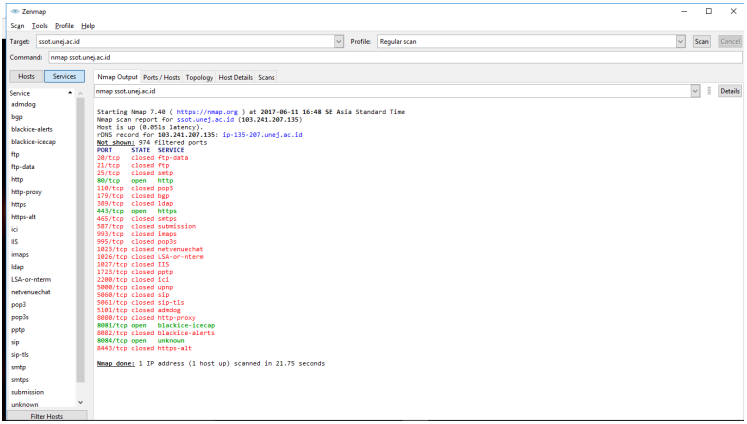

History
Search
Alerts
Output
Spider
Active Scan
Alerts (4)
X-Frame-Options Header Not Set (2)
Incomplete or No Cache-control and Pragma HTTP Header Set (3)
Web Browser XSS Protection Not Enabled (5)
X-Content-Type-Options Header Missing (10)

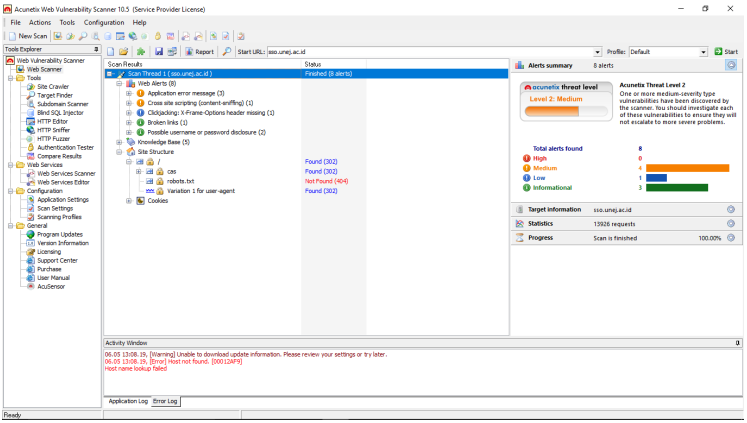

History
Search
Alerts
Output
Active Scan
Alerts (6)
X-Frame-Options Header Not Set
Cookie No HttpOnly Flag (2)
Cookie Without Secure Flag (2)
Incomplete or No Cache-control and Pragma HTTP Header Set (5)
Web Browser XSS Protection Not Enabled (4)
X-Content-Type-Options Header Missing (10)

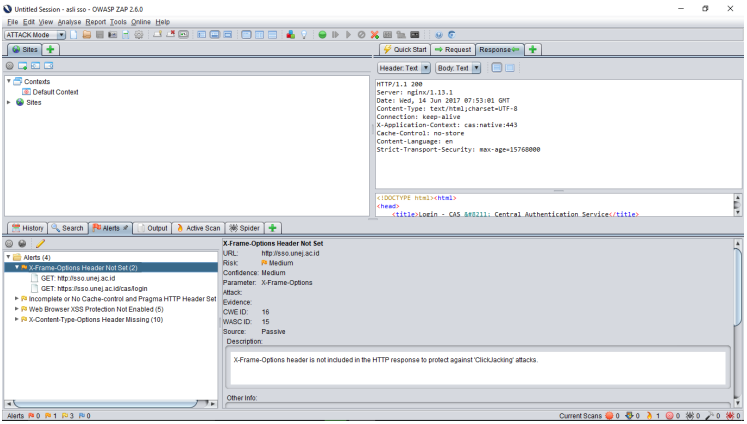

Request | Text Only
Method: POST
Protocol: HTTP/1.1
URL: /cas/login
Edit Request Variables
Request Headers
Request Data
Header Name
Header Value
Content-Length
2231
Content-Type
application/x-www-form-urlencoded
Referer
sso.unej.ac.id
Cookie
JSESSIONID=D66236D6C173D8E31A69B2D9F237C4
Host
sso.unej.ac.id
Connection
Keep-alive
Accept-Encoding
gzip,deflate
User-Agent
Mozilla/5.0 (Windows NT 6.1; WOW64) AppleWebKit/537...
Acunetix-Product
WVS/10.0 (Acunetix Web Vulnerability Scanner - Free Edi...
Acunetix-Scanning-agreement
Third Party Scanning PROHIBITED
submit=LOGIN&execution=d0c26371-6406-4757-a2e1-58f59b1aba63_ZX1kaGJN
Response Headers
Response Data
View Page
Structure Analysis
{"timestamp":1497425223985,"status":500,"error":"Internal Server Error","exception":"org.springframework.webflow.engine.NoMatchingTransitionException","message":"No transition found on occurence of event '12345'\"\\'\\'');;]*\u0000{'r\n<\u0000>¿½'\uD83D\uDCA9' in state 'viewLoginForm' of flow 'login' -- valid transitional criteria are array[submit] -- likely programmer error, check the set of TransitionCriteria for this state","trace":"org.springframework.webflow.engine.NoMatchingTransitionException: No transition found on occurence of event '12345'\"\\'\\'');;]*\u0000{'r\n<\u0000>¿½'\uD83D\uDCA9' in state 'viewLoginForm' of flow 'login' -- valid transitional criteria are array[submit] -- likely programmer error, check the set of TransitionCriteria for this state\n\tat org.springframework.webflow.engine.TransitionableState.getRequiredTransition(TransitionableState.java:90)\n\tat
org.springframework.webflow.engine.TransitionableState.handleEvent(TransitionableState.java:116)\n\tat org.springframework.webflow.engine.Flow.handleEvent(Flow.java:547)\n\tat
org.springframework.webflow.engine.impl.FlowExecutionImpl.handleEvent(FlowExecutionImpl.java:390)\n\tat
org.springframework.webflow.engine.impl.RequestControlContextImpl.handleEvent(RequestControlContextImpl.java:210)\n\tat
org.springframework.webflow.engine.ViewState.handleEvent(ViewState.java:231)\n\tat org.springframework.webflow.engine.ViewState.resume(ViewState.java:195)\n\tat
org.springframework.webflow.engine.Flow.resume(Flow.java:537)\n\tat org.springframework.webflow.engine.impl.FlowExecutionImpl.resume(FlowExecutionImpl.java:259)\n\tat
org.springframework.webflow.executor.FlowExecutorImpl.resumeExecution(FlowExecutorImpl.java:169)\n\tat sun.reflect.GeneratedMethodAccessor360.invoke(Unknown Source)\n\tat

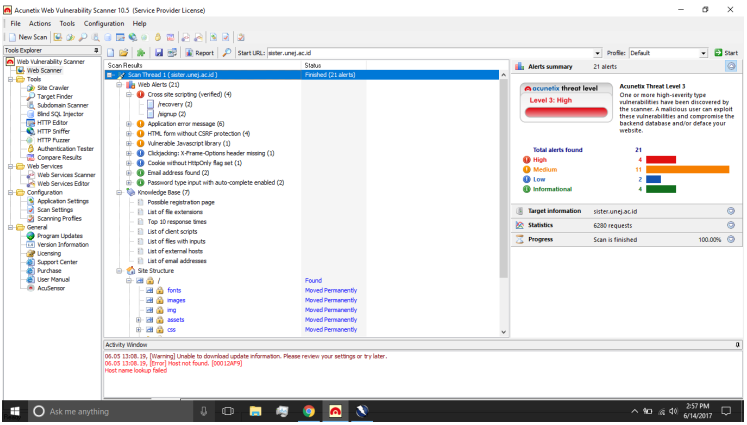

Request Headers
Request Data
Header Name
Header Value
Content-Length
173
Content-Type
application/x-www-form-urlencoded
Referer
http://ssot.unej.ac.id:80/
Cookie
JSESSIONID=033982E2D3072E681A6469285A60B3A7
Host
ssot.unej.ac.id
Connection
Keep-alive
Accept-Encoding
gzip,deflate
User-Agent
Mozilla/5.0 (Windows NT 6.1; WOW64) AppleWebKit/537...
Acunetix-Product
WVS/10.0 (Acunetix Web Vulnerability Scanner - Free Edi...
Acunetix-Scanning-agreement
Third Party Scanning PROHIBITED
submit=LOGIN&execution=<h1>XSS
BERHASIL</h1>&geolocation&password=g00dPa%24%24w0rDzremember
ername=tgvejqpw&_eventId=1%22()%26%25<acx><ScRiPt%20>ym09(9594)</ScRiPt>
Response Headers
Response Data
View Page
Structure Analysis
{"timestamp":1497195423277,"status":500,"error":"Internal Server Error","exception":"org.springframework.webflow.execution.repository.BadlyFormattedFlowExecutionKeyException","message":"Badly formatted flow execution key '
XSS BERHASIL
', the expected format is '_'","trace":"org.springframework.webflow.execution.repository.BadlyFormattedFlowExecutionKeyException: Badly formatted flow execution key '
XSS BERHASIL

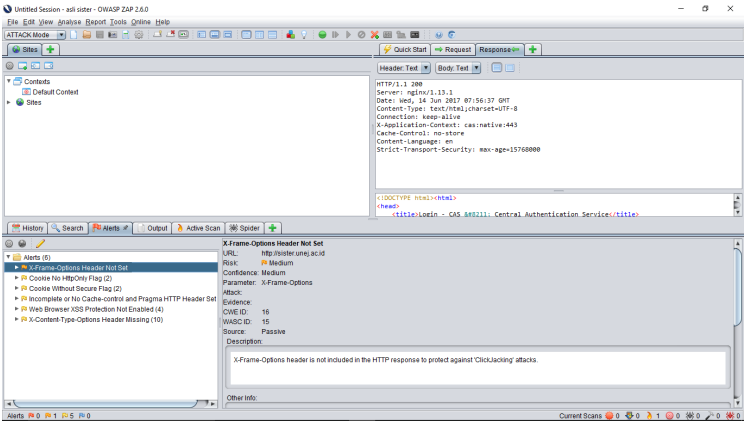

Secure
https://ssot.unej.ac.id/cas/login
SISTER SSO
UNIVERSITAS JEMBER
Sistem menjalani backup otomatis setiap hari pukul 00.00-01.00 WIB . Selama waktu tersebut website tidak bisa diakses!
Enter your Username and Password
Invalid credentials.
Username:
"<script>alert(1)</script>"
Password:
Remember Me
LOGIN
clear
SISTER
Sistem Informasi Terpadu Universitas Jember
Copyright © UPT TI UNEJ
E-learning
Modular Object-Oriented Dynamic Learning Environment (MOODLE)
Copyright © 1999 Martin Dougiamas and others
Simangga
Sistem Informasi Manajemen Anggaran Universitas Jember
Copyright © BAPSI UNEJ
Simkeu
Sistem Informasi Keuangan Universitas Jember
Copyright © Keuangan UNEJ
Forum Blogger UNEJ
weblunej.ac.id
UNEJ
SIKD
Sistem Informasi Kearsipan Dinamis
Copyright © ANRI
Lupa Password
Manual Sister untuk Mahasiswa
Cara Koneksi Wifi.ID
Manual BLOG UNEJ
Sehubungan dengan berakhirnya masa trial akses wifi.id UNEJ, bagi mahasiswa yang ingin memperpanjang langganan wifi.id dapat melakukan pembayaran sebesar 15.000/bulan melalui BNI Kampus.
Copyright © 2005-2016 Apereo, Inc.
Powered by


Zenmap
Scan Tools Profile Help
Target: ssot.unej.ac.id
Profile: Regular scan
Scan
Cancel
Command: nmap ssot.unej.ac.id
Hosts
Services
Nmap Output
Ports / Hosts
Topology
Host Details
Scans
nmap ssot.unej.ac.id
Details
Service
admdog
bgp
blackice-alerts
blackice-icecap
ftp
ftp-data
http
http-proxy
https
https-alt
icl
IIS
imaps
ldap
LSA-or-nterm
netvenuechat
pop3
pop3s
pptp
sip
sip-tls
smtp
smtps
submission
unknown
Filter Hosts
Starting Nmap 7.40 (https://nmap.org) at 2017-06-11 16:48 SE Asia Standard Time
Nmap scan report for ssot.unej.ac.id (103.241.207.135)
Host is up (0.051s latency).
rDNS record for 103.241.207.135: ip-135-207.unej.ac.id
Not shown: 974 filtered ports
PORT STATE SERVICE
20/tcp closed ftp-data
21/tcp closed ftp
25/tcp closed smtp
80/tcp open http
110/tcp closed pop3
179/tcp closed bgp
389/tcp closed ldap
443/tcp open https
465/tcp closed smtps
587/tcp closed submission
993/tcp closed imaps
995/tcp closed pop3s
1023/tcp closed netvenuechat
1026/tcp closed LSA-or-nterm
1027/tcp closed IIS
1723/tcp closed pptp
2200/tcp closed icl
5000/tcp closed upnp
5060/tcp closed sip
5061/tcp closed sip-tls
5101/tcp closed admdog
8000/tcp closed http-proxy
8081/tcp open blackice-icecap
8082/tcp closed blackice-alerts
8084/tcp open unknown
8443/tcp closed https-alt
Nmap done: 1 IP address (1 host up) scanned in 21.75 seconds


Acunetix Web Vulnerability Scanner 10.5 (Service Provider License)
File Actions Tools Configuration Help
New Scan
Tools Explorer
Web Vulnerability Scanner
Web Scanner
Tools
Site Crawler
Target Finder
Subdomain Scanner
Blind SQL Injector
HTTP Editor
HTTP Sniffer
HTTP Fuzzer
Authentication Tester
Compare Results
Web Services
Web Services Scanner
Web Services Editor
Configuration
Application Settings
Scan Settings
Scanning Profiles
General
Program Updates
Version Information
Licensing
Support Center
Purchase
User Manual
AcuSensor
Report
Start URL: sso.unej.ac.id
Profile: Default
Start
Scan Results
Status
Scan Thread 1 (sso.unej.ac.id)
Finished (8 alerts)
Web Alerts (8)
Application error message (3)
Cross site scripting (content-sniffing) (1)
Clickjacking: X-Frame-Options header missing (1)
Broken links (1)
Possible username or password disclosure (2)
Knowledge Base (5)
Site Structure
/
Found (302)
cas
Found (302)
robots.txt
Not Found (404)
Variation 1 for user-agent
Found (302)
Cookies
Alerts summary
8 alerts
acunetix threat level
Level 2: Medium
Acunetix Threat Level 2
One or more medium-severity type vulnerabilities have been discovered by the scanner. You should investigate each of these vulnerabilities to ensure they will not escalate to more severe problems.
Total alerts found
8
High
0
Medium
4
Low
1
Informational
3
Target information
sso.unej.ac.id
Statistics
13926 requests
Progress
Scan is finished
100.00%
Activity Window
06.05 13:08.19, [Warning] Unable to download update information. Please review your settings or try later.
06.05 13:08.19, [Error] Host not found. [00012AF9]
Host name lookup failed
Application Log
Error Log
Ready


Untitled Session - asli sso - OWASP ZAP 2.6.0
File Edit View Analyse Report Tools Online Help
ATTACK Mode
Sites
Quick Start
Request
Response
Header: Text
Body: Text
Contexts
Default Context
Sites
HTTP/1.1 200
Server: nginx/1.13.1
Date: Wed, 14 Jun 2017 07:53:01 GMT
Content-Type: text/html;charset=UTF-8
Connection: keep-alive
X-Application-Context: cas:native:443
Cache-Control: no-store
Content-Language: en
Strict-Transport-Security: max-age=15768000
<!DOCTYPE html><html>
<head>
<title>Login - CAS – Central Authentication Service</title>
History
Search
Alerts
Output
Active Scan
Spider
Alerts (4)
X-Frame-Options Header Not Set (2)
GET: http://sso.unej.ac.id
GET: https://sso.unej.ac.id/cas/login
Incomplete or No Cache-control and Pragma HTTP Header Set
Web Browser XSS Protection Not Enabled (5)
X-Content-Type-Options Header Missing (10)
X-Frame-Options Header Not Set
URL: http://sso.unej.ac.id
Risk: Medium
Confidence: Medium
Parameter: X-Frame-Options
Attack:
Evidence:
CWE ID: 16
WASC ID: 15
Source: Passive
Description:
X-Frame-Options header is not included in the HTTP response to protect against 'ClickJacking' attacks.
Other Info:
Alerts
Current Scans


Acunetix Web Vulnerability Scanner 10.5 (Service Provider License)
File Actions Tools Configuration Help
New Scan
Tools Explorer
Web Vulnerability Scanner
Web Scanner
Tools
Site Crawler
Target Finder
Subdomain Scanner
Blind SQL Injector
HTTP Editor
HTTP Sniffer
HTTP Fuzzer
Authentication Tester
Compare Results
Web Services
Web Services Scanner
Web Services Editor
Configuration
Application Settings
Scan Settings
Scanning Profiles
General
Program Updates
Version Information
Licensing
Support Center
Purchase
User Manual
AcuSensor
Report
Start URL: sister.unej.ac.id
Profile: Default
Start
Scan Results
Status
Scan Thread 1 [sister.unej.ac.id]
Finished [21 alerts]
Web Alerts (21)
Cross site scripting (verified) (4)
/recovery (2)
/signup (2)
Application error message (6)
HTML form without CSRF protection (4)
Vulnerable Javascript library (1)
Clickjacking: X-Frame-Options header missing (1)
Cookie without HttpOnly flag set (1)
Email address found (2)
Password type input with auto-complete enabled (2)
Knowledge Base (7)
Possible registration page
List of file extensions
Top 10 response times
List of client scripts
List of files with inputs
List of external hosts
List of email addresses
Site Structure
/
Found
fonts
Moved Permanently
images
Moved Permanently
img
Moved Permanently
assets
Moved Permanently
css
Moved Permanently
Alerts summary
21 alerts
acunetix threat level
Level 3: High
Acunetix Threat Level 3
One or more high-severity type vulnerabilities have been discovered by the scanner. A malicious user can exploit these vulnerabilities and compromise the backend database and/or deface your website.
Total alerts found
21
High
4
Medium
11
Low
2
Informational
4
Target information
sister.unej.ac.id
Statistics
6280 requests
Progress
Scan is finished
100.00%
Activity Window
06.05 13:08.35, [Warning] Unable to download update information. Please review your settings or try later.
06.05 13:08.35, [Error] Host not found. [00012AF9]
Host name lookup failed
Ask me anything
2:57 PM
6/14/2017


Untitled Session - asli sister - OWASP ZAP 2.6.0
File Edit View Analyse Report Tools Online Help
ATTACK Mode
Sites
Contexts
Default Context
Sites
Quick Start
Request
Response
Header: Text
Body: Text
HTTP/1.1 200
Server: nginx/1.13.1
Date: Wed, 14 Jun 2017 07:56:37 GMT
Content-Type: text/html;charset=UTF-8
Connection: keep-alive
X-Application-Context: cas:native:443
Cache-Control: no-store
Content-Language: en
Strict-Transport-Security: max-age=15768000
<!DOCTYPE html><html>
<head>
<title>Login - CAS – Central Authentication Service</title>
History
Search
Alerts
Output
Active Scan
Spider
Alerts (6)
X-Frame-Options Header Not Set
Cookie No HttpOnly Flag (2)
Cookie Without Secure Flag (2)
Incomplete or No Cache-control and Pragma HTTP Header Set
Web Browser XSS Protection Not Enabled (4)
X-Content-Type-Options Header Missing (10)
X-Frame-Options Header Not Set
URL: http://siste.unej.ac.id
Risk: Medium
Confidence: Medium
Parameter: X-Frame-Options
Attack:
Evidence:
CWE ID: 16
WASC ID: 15
Source: Passive
Description:
X-Frame-Options header is not included in the HTTP response to protect against 'ClickJacking' attacks.
Other Info:
Alerts
Current Scans